Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Algebra 277 (2004) 36–72

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Quadratic pairs

Andrew Chermak

Department of Mathematics, Kansas State University, Manhattan, KS 66502, USA

Received 14 May 2002

Available online 30 April 2004

Communicated by Gernot Stroth

Introduction

This paper revisits (and completes) the work of John Thompson and Chat-Yin Ho (cf. [9,17]) from the early 1970s, on the "Quadratic pairs." Thus, we will be concerned with the following situation.

Hypothesis 1.0. G is a finite group, p is an odd prime, and V is a faithful, irreducible module for G over the field $\mathbb{F}_p$ of p elements. Further, there is a subgroup A of G such that $G = \langle A^G \rangle$ and such that $[V, A, A] = 0$.

Recall that a group H is *quasisimple* if $H = [H, H]$ and $H/Z(H)$ is simple. In [3] the author considered the case in which, in addition to Hypothesis 1.0, it is assumed that G has no quasisimple subnormal subgroups. (Such subgroups are the *components* of G.) In this paper, we take up the alternative case, in which G has at least one component. By Lemma 1.4 in [3] this amounts to making the following stronger hypothesis.

Hypothesis 1.1. In addition to Hypothesis 1.0, we assume that there is a normal, quasisimple subgroup H of G, such that $C_G(H) = Z(G)$.

As an addendum to Hypothesis 1.1 we assume that, in fact, $H/Z(H)$ is one of the groups given by the Classification of the Finite Simple Groups. That is to say, $H/Z(H)$ is isomorphic to an alternating group, a group of Lie type, or one of twenty-six sporadic groups. We assume also that we have complete information about the Schur multipliers of the finite simple groups, so that not only $H/Z(H)$, but H itself, is a "known" group. We shall prove the following result.

E-mail address: chermak@ksu.edu.

0021-8693/$ – see front matter
doi:10.1016/S0021-8693(03)00334-X

Theorem A. *Assume Hypothesis* 1.1 *and the above addendum. Then* $Z(G) \leqslant H$, *and either* $G = H$ *is a group of Lie type in characteristic* p, *or* $|A| = p = 3$, *and one of the following holds.*

(a) $G \cong PGU(n, 2)$, $n \geqslant 5$,
(b) $|Z(G)| = 2$, $\overline{G} \cong Alt(n)$, $n \geqslant 5$ *and* $n \neq 6$, *or*
(c) $|Z(G)| = 2$, *and* $\overline{G}$ *is isomorphic to* $D_4(2)$, $G_2(4)$, $Sp(6, 2)$, Co_1, *Suz, or* J_2.

We rely largely on [6] for information about "known" simple or quasisimple groups, but we have made an attempt to keep to a minimum the amount of detailed information that we draw upon, and to rely on general principles as far as is practicable. For the sporadic groups, by their very nature (or by the nature of the current state of understanding of these groups) we are forced to take an opportunistic approach, but we can get by with information on conjugacy classes, centralizers, Schur multipliers, and the fact that none of the sporadic groups have outer automorphisms of odd order. That is, we require only "basic" information, such as can be found either in the ATLAS of Finite Groups [4] or in Table 5.3 in [6]. Concerning the simple groups of Lie type, the situation is turned on its head, and we have made it a point to avoid appealing to the detailed information (provided in [6] and elsewhere) concerning the structure of centralizers, and to rely only on information derivable from the most basic results relating the simple groups of Lie type to simple algebraic groups, and from the Coxeter diagrams of these various groups. As has already been mentioned, we take for granted the determination of the Schur multipliers. Aside from that, we need the theorem of Borel and Tits which states that p-local subgroups of simple groups of Lie type in characteristic p are contained in parabolic subgroups, and are p-constrained, and we need some results, due to Steinberg, concerning automorphisms of the groups of Lie type. Other properties of the groups of Lie type that will be needed here will be developed in Section 3, below.

Whenever Hypothesis 1.1 is in effect, we denote by H the unique normal, quasisimple subgroup of G, and we set $\overline{G} = G/Z(G)$. Further, we adopt the "bar convention," whereby the image in $\overline{G}$ of a subgroup X of G is denoted $\overline{X}$.

By a *quadratic module* for a group X, we mean a module U such that $[U, A, A] = 0$ for some non-identity subgroup A of X such that $X = \langle A^X \rangle$. We then say that A is a *quadratic subgroup* of X.

In the exceptional cases (a) through (c) of Theorem A, we determine the possible conjugacy classes of quadratic subgroups of order 3. The result is as follows.

Theorem B. *Assume Hypothesis* 1.1, *and assume that* G *is not a group of Lie type in characteristic* p. *Let* A *be a quadratic subgroup of order* 3 *in* G.

(a) *Suppose that* $G = PGU(n, 2)$, $n \geqslant 5$. *Let* $\phi : GU(n, 2) \to PGU(n, 2)$ *be the canonical homomorphism, and let* U *be the natural module for* $GU(n, 2)$ *over the field* $\mathbb{F}_4$. *Then there is an element* a^* *of* $GU(n, 2)$ *with* $\langle \phi(a^*) \rangle = A$, *such that* $C_U(a^*)$ *has codimension* 1 *in* U.
(b) *If* $\overline{G} \cong Alt(n)$, $n \neq 6$, *then* $\overline{A}$ *is generated by a* 3*-cycle in* $\overline{G}$.

(c) *If* $\overline{G} \cong D_4(2)$ *then* $C_{\overline{G}}(\overline{A}) \cong 3 \times U_4(2)$, *and* A *lies in a maximal subgroup* M *of* G *such that* $O_2(M)$ *is an extraspecial* 2*-group of order* 2^7, *with* $M/O_2(M) \cong L_4(2)$, *and such that* $[O_2(M), A]$ *is a quaternion group.*
(d) *If* $\overline{G} \cong G_2(4)$ *then* $C_{\overline{G}}(\overline{A}) \cong SL(3, 4)$.
(e) *If* $\overline{G} \cong Sp(6, 2)$ *then* $C_{\overline{G}}(\overline{A}) \cong 3 \times Sp(4, 2)$.
(f) *If* $\overline{G} \cong J_2$ *then* $C_{\overline{G}}(\overline{A}) \cong 3^{\cdot}Alt(6)$.
(g) *If* $\overline{G} \cong Suz$ *then* $C_{\overline{G}}(\overline{A}) \cong 3^{\cdot}U_4(3)$.
(h) *If* $\overline{G} \cong Co_1$ *then* $C_{\overline{G}}(\overline{A}) \cong 3^{\cdot}Suz$.

Moreover, in every case except (c), *the conjugacy class of* A *in* G *is uniquely determined by the given conditions. In case* (c) *the class of* A *is uniquely determined up to conjugacy in* $Aut(G)$.

We remark, in connection with Theorem A, that there are descending chains of groups

$$2^{\cdot}Co_1 \geqslant 6^{\cdot}Suz \geqslant 2^{\cdot}G_2(4) \geqslant 2^{\cdot}J_2,$$

and

$$2^{\cdot}Co_1 \geqslant 2^{\cdot}D_4(2) \geqslant 2^{\cdot}Sp(6, 2).$$

Denote by Λ the (24-dimensional) Leech Lattice, with automorphism group $2^{\cdot}Co_1$. We will show in Section 9, below, that $\Lambda/3\Lambda$ is a quadratic module for $2^{\cdot}Co_1$, and a quadratic module also for each of the groups in each of the above chains of subgroups. Thus, all of the groups listed in part (c) of Theorem A possess quadratic modules in characteristic 3.

Also, the groups G listed in parts (a) and (b) of Theorem A have quadratic modules in characteristic 3. For $2^{\cdot}Alt(n)$ such modules have been classified in [10]. For the unitary groups in characteristic 2, and also for the exceptional groups in (c), a complete determination of the quadratic modules appears in [8]. The quadratic modules for the groups of Lie type in characteristic p, p odd, were determined long ago, in [11].

The following corollary to Theorems A and B is useful for certain applications.

Corollary C. *Assume Hypothesis* 1.1, *and assume that* G *is not a group of Lie type in characteristic* p. *Assume also that there exists a quadratic subgroup* A *of* G *such that* $|A|^2 \geqslant |V/C_V(A)|$. *Then* $p = 3$, $G \cong SL(2, 5)$, *and* V *is a natural* $SL(2, 9)$*-module for* G.

In proving Theorem A, we can reduce immediately to the case where $G = HA$, as the following lemma shows.

Lemma 1.2. *Let* G *be a minimal counter-example to Theorem* A. *Then* $G = HA$.

Proof. Set $G_0 = HA$. As H is quasisimple we have $G_0 = \langle A^{G_0} \rangle$, and evidently V is a quadratic module for G_0. By Clifford's theorem, there exists an irreducible H-submodule U of V on which H acts faithfully. Then also H acts faithfully on any irreducible G_0-submodule V_0 of $\langle U^A \rangle$. As V is irreducible for G, $Z(G)$ is a $3'$-group, and then

since $C_G(H) = Z(G)$, by Hypothesis 1.1, we have $C_{G_0}(V_0) = 1$. Thus, Hypothesis 1.1 is satisfied by G_0 and V_0 in place of G and V. Suppose now that $G \neq G_0$. Then $A \not\leq H$, and since G is a minimal counter-example to Theorem A, we may appeal to Theorem A for the structure of G_0. The condition that A not be contained in H then yields $G_0 \cong PGU(n, 2)$, where 3 divides n. But then $G_0 \cong Aut(H)$, and so $G = C_G(H)G_0$. Hypothesis 1.1 then yields $G = Z(G)G_0$. As $G = \langle A^G \rangle = [G, A]A$, it follows that $G = G_0A$, and so $G = G_0$. □

The structure of this paper is as follows. We begin, in Section 2, by collecting together some general results about quadratic action, including a lemma of Meierfrankenfeld (Lemma 2.8, below) which gives a useful characterization of the groups $SL(2, p)$ for $p > 3$.

Section 3 concerns properties of quasisimple groups of Lie type. As indicated above, we have found it convenient to draw on [6] for basic background material. From this background we obtain results on automorphisms, on centralizers, and on the action of certain automorphisms on Schur multipliers.

In Section 4 we use the results of Section 3 in order to show that, if $\overline{G}$ is a group of Lie type (possibly of characteristic p) then $\bar{a}$ induces an inner-diagonal automorphism on $\overline{G}$. We also show that if $\overline{G}$ is an alternating group, then $\overline{A}$ is generated by a 3-cycle, and $|Z(G)| = 2$. Thus, in the succeeding sections, we need only be concerned with groups of Lie type (possibly extended above by diagonal automorphisms) in characteristic different from p, and with sporadic groups.

Section 5 provides a quick treatment of the case where p is greater than 3. (Of course, the result here is not new. See [12] for a treatment which is based on Aschbacher's classification of groups of Lie type in odd characteristic. Much more recently, one has Timmesfeld's work [18], where the groups are not assumed to be finite, but in which the question addressed by Lemma 2.8 below is left open.) From then on, we assume that $p = 3$, and Section 6 is devoted to the case where $\overline{H}$ is of Lie type in characteristic different from 3. Section 7 treats the case where $p = 3$ and $\overline{H}$ is a sporadic group. Finally, Sections 8 and 9 provide proofs for Theorem B and Corollary C, and establish that all of the "exceptional" groups that arise in Theorem A do indeed have quadratic modules.

It should be emphasized that this paper should in no way be construed as somehow finessing the work of Thompson and Ho. The work of Thompson was begun before the Classification was anywhere within sight, and before there was even any strong reason to believe that only a small number of finite simple groups remained to be discovered. Thompson's work, and that of Ho, may be understood as an attempt to continue the momentum towards the Classification that had begun with the Odd Order Paper and the N-Group Paper. Their work was dropped when a powerful program leading to the Classification began to take shape. On the other hand, a new approach to at least one aspect of the Classification (concerning groups having a "generic prime characteristic") is currently developing, under the leadership of Meierfrankenfeld. The determination of certain kinds of quadratic groups and modules, in arbitrary prime characteristic, forms one of the tools that are needed for the Meierfrankenfeld program.

We wish to end this introduction with some further remarks concerning the earlier treatments (in [9,17], and [16]) of various aspects of the Quadratic Pairs. All of these papers (and the more recent [18]) begin with the notion of a *root group*, and although that

notion plays no direct role in the present work, it may be instructive to review the definition. Thus, given an odd prime p and a quadratic pair (G, V) (i.e., a pair for which some A exists satisfying Hypothesis 1, above), denote by $\mathcal{Q}$ the set of non-identity elements of G which act quadratically on V, and for any $x \in \mathcal{Q}$ set $d(x) = \dim_{\mathbb{F}_p}([V, x])$. Let d be the minimum over all $d(x)$ for $x \in \mathcal{Q}$, and set $\mathcal{Q}_d = \{x \in \mathcal{Q}\colon\ d(x) = d\}$. For any $x \in \mathcal{Q}_d$, set

$$E(x) = \big\langle y \in \mathcal{Q}\colon\ C_V(x) = C_V(y) \text{ and } [V, x] = [V, y]\big\rangle \cup \{1\}.$$

Then $E(x)$ is an elementary abelian p-group, called a *root group* of G. In the case that $p > 3$, Thompson showed that any pair X and Y of non-commuting root groups generates a subgroup of G isomorphic to $SL(2, q)$, where $q = |E(x)|$ for any $x \in \mathcal{Q}$. In particular, there is a unique involution $t \in \langle X, Y\rangle$ in this situation, and one may approach the identification of G by means of the centralizers of such involutions t. This is essentially the approach in [16] and in [18].

The situation for $p = 3$ is more complicated. In particular, there are examples for which $F^*(G)$ is a 2-group, and there are examples where $F^*(G)$ is quasisimple and unequal to G. Ho's achievement, in a series of papers culminating in [9], was to classify the quasisimple groups G for which there is a quadratic pair (G, V) for $p = 3$, and in which there exists a root group of order greater than 3, or in which no two root groups generate a subgroup of G which is isomorphic to $SL(2, 3) \times \mathbb{Z}_3$. The assumption that G be quasisimple has the unfortunate aspect of leaving the groups $PGU(n, 2)$ out of consideration, for n divisible by 3. Thus, one way to proceed with a classification of quadratic pairs for $p = 3$ would be to build on Ho's work, where it is likely that the simplicity hypothesis is inessential, and to analyze the case where $SL(2, 3) \times \mathbb{Z}_3$ appears as a subgroup of G which is generated by two root groups. (That this case never occurs, in fact, is a consequence of Theorems A and B here, and of [3].) If such an approach, without using the CFSG, could be successfully completed, the result would be a welcome addition to this chapter of finite group theory.

2. Quadratic groups

Lemma 2.1. *Let G be a finite group generated by two elements x_1 and x_2 of odd prime order p. Suppose that there exists a faithful, irreducible G-module V over $\mathbb{F}_p$, with $[V, x_i, x_i] = 0$ for both $i = 1$ and 2. Then one of the following holds*:

(i) *$G \cong SL(2, p^n)$ for some n, and V is a natural module for G, or*
(ii) *$p = 3$, $G \cong SL(2, 5)$, and V is a natural $SL(2, 9)$-module for G.*

Proof. Let F be a splitting field for G over $\mathbb{F}_p$, and put $\widetilde{V} = F \otimes V$. Put $\Gamma = Aut(F)$. Then $\widetilde{V}$ is an irreducible module for $\Gamma \times G$, by [1, Result 25.7]. Let U be an irreducible $F[G]$-submodule of $\widetilde{V}$. There is then a finite subset Σ of $Aut(F)$, containing the identity automorphism, such that:

$$\widetilde{V} = \bigoplus \big\{U^\sigma\colon\ \sigma \in \Sigma\big\}.$$

Since $C_G(\widetilde{V}) = 1$, we then have $C_G(U) = 1$. Thus, U is a faithful, irreducible $F[G]$-module. Theorem 3.8.1 of [5] then says that G contains a subgroup isomorphic to $SL(2, p)$. But the point is that a much stronger statement is actually proved. Namely, the argument of [5, Theorem 3.8.1] shows that $\dim_F(U) = 2$, and that, relative to a suitable basis of U, the generators x_1 and x_2 of G have the matrix form:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$$

for some $\lambda \in F$. A theorem of L.E. Dickson (Theorem 2.8.4 in [5]) then implies that either $G \cong SL(2, p^n)$, where λ is a primitive $(p^n - 1)$th-root of unity; or else $p = 3$, $\lambda \in \mathbb{F}_9$, and $G \cong SL(2, 5)$. Moreover, U is then seen to be irreducible as a G-module over $\mathbb{F}_p$, and hence U is isomorphic to V as $\mathbb{F}_p[G]$-modules. This yields the lemma. □

Lemma 2.2. *Let $X \cong SL_2(q)$, let T be a Sylow p-subgroup of X, and let V be a module for X over $\mathbb{F}_p$, such that $[V, T, T] = 0$ and such that $[V, O^p(X)] \neq 0$. Then $[V/C_V(O^p(X)), O^p(X)]$ is a direct sum of natural modules for X.*

Proof. Without loss, we may assume that $C_V(X) = 0$. Set $B = N_X(T)$, let H be a complement to T in B, and let $s \in N_X(H) - H$. Let U be an irreducible H-invariant subspace of $C_V(T)$. Then $|U| \leqslant q$. We have $X = B \cup BsB$, so

$$W = U + U^{sB} = U + U^{sT} = U + U^s + \big[U^s, T\big].$$

As $[V, T] \leqslant C_V(T)$ we conclude that $|W/C_W(T)| \leqslant |U|$, and since X is generated by two conjugates of T we conclude that $|W| \leqslant |U|^2$. Let $0 \neq v \in U^s$. Then $W = U \oplus U^s$, and since $X = \langle T^s, t\rangle$ for any $t \in T^{\#}$ we have $C_T(v) = 1$. Thus $U = [v, T]$ and $|U| = |T| = q$. This shows that $|W| = q^2$ and that $End_H(U) = \mathbb{F}_q$. Then $End_W(X) = \mathbb{F}_q$ and W is a natural module for X. As $[V, O^p(X)] \leqslant [V, T] + [V, T^s]$, the lemma follows. □

Lemma 2.3. *Let p be an odd prime, let V be a vector space of dimension 4 over $\mathbb{F}_p$, and let U be a subspace of V of dimension 2. Let H be a subgroup of $GL(V)$ which leaves U invariant, and assume that H has the following two properties.*

(1) $O_p(H) = C_H(U) = C_H(V/U)$,
(2) $H/O_p(H) \cong SL(2, p)$.

Then the following hold.

(a) *If there exists an element a of order p in $H - O_p(H)$, with $[V, a, a] = 0$, then there is a complement L to $O_p(H)$ in H, containing a. For any such complement L we have $V = U \oplus U_1$ for some L-submodule U_1 of V.*
(b) *If $p > 3$ and there exists a complement L to $O_p(H)$ in H, then $[V, b, b] = 0$ for any element b of order p in L.*

Proof. Set $N = N_{GL(V)}(U)$, $R = O_p(N)$, $\overline{N} = N/R$, and $M = O^{p'}(N)$. Then $\overline{M} \cong SL(2, p) \times SL(2, p)$ and R is a natural $\Omega_4^+(p)$-module for $\overline{M}$. Here $\overline{H}$ is a "diagonal" copy of $SL(2, p)$ in $\overline{M}$. That is, $\overline{H} \cong SL(2, p)$ and $\overline{H}$ is not a direct factor of $\overline{M}$. If $p = 3$ we observe that also $O_2(\overline{H})$ acts non-trivially on both U and V/U. For any p, the above conditions determine $\overline{H}$ up to conjugacy in $\overline{N}$, and we may therefore identify RH with the subgroup of $GL(4, p)$ consisting of all matrices of the form

$$\begin{pmatrix} X & A \\ 0 & X \end{pmatrix}, \tag{$*$}$$

where $X \in SL(2, p)$ and where A is an arbitrary 2×2 matrix over $\mathbb{F}_p$. Set $R_0 = [R, H]$. Then R_0 is a natural $\Omega_3(p)$-module for $\overline{H}$, $|C_R(H)| = p$, and $R = R_0 \times C_R(H)$. Let L_0 be the subgroup of RH consisting of those matrices for which $A = 0$. Let c be an element of order p in $R_0L_0 - R_0$, and set $T = R_0\langle c\rangle$. Then T is a Sylow p-subgroup of R_0L_0, and we have $[R_0, c, c, c] = 0 \neq [R_0, c, c]$. It follows that for any $x \in R_0 - [R_0, c]$, we have $|xc| = p^2$, and that $\Omega_1(T) = \langle c^{R_0}\rangle$ is an extraspecial group of order p^3 and exponent p. Denote by $\mathcal{Y}$ the set of subgroups of $\Omega_1(T)$ which are not contained in R_0. Then R_0 acts transitively on $\{Y \in \mathcal{Y}\colon |Y| = p^2\}$. Also, for any $Y \in \mathcal{Y}$ with $|Y| = p^2$, $\Omega_1(T)$ acts transitively on the set of cyclic subgroups of Y which lie in $\mathcal{Y}$. Thus, all subgroups of order p in T which are not contained in R_0 are conjugate in T.

Let d be an element of order p in $C_R(H)T - T$. Then $d = cz$ where c is as above, and where $1 \neq z \in C_R(H)$. Conjugating by T, we may take $c \in L_0$. One observes that c acts quadratically on V, and that cz is of the form

$$\begin{pmatrix} 1 & \lambda & \mu & 0 \\ 0 & 1 & 0 & \mu \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where λ and μ are non-zero. Then cz does not act quadratically on V. Thus, we have shown:

Every quadratic element of $X - R$ of order p lies in R_0L_0, and is conjugate via R_0 to an element of L_0. (1)

Suppose that $p > 3$ and that there exists a complement L to $O_p(H)$ in H. Then $L \leqslant [X, X] = R_0L_0 = R_0L$, and by (1), every element of order p in L is quadratic. Thus, (b) holds.

Now suppose instead that there is a quadratic element a of order p in $H - O_p(H)$. If $R_0 \leqslant H$, then (1) implies that $\langle a^H\rangle = R_0L_0$, and there is an R_0-conjugate L of L_0 containing a. Suppose that $R_0 \not\leqslant H$. Then $H \cong SL(2, p)$ or $SL(2, p) \times \mathbb{Z}_p$, and in either case a lies in a subgroup L of H with $L \cong SL(2, p)$. In any case, Lemma 2.2 shows that V is decomposable as a module for L, and so (a) holds. □

Lemma 2.4. *Let G be a finite group, p an odd prime, and V a faithful $\mathbb{F}_p[G]$-module. Suppose that we are given an element $a \in G - O_p(G)$ with $[V, a, a] = 0$. Then there is a subgroup $H = \langle a^H\rangle$ of G having the following properties*:

(a) $H \cong SL(2, p)$, *or else* $p > 3$ *and* $H \cong \mathbb{Z}_p \times SL(2, p)$.
(b) $V = [V, H] \oplus C_V(O^p(H))$, *and* $[V, H]$ *is a direct sum of natural* $SL(2, p)$*-modules for* H.

In particular, there exists an element b *of order* p *in* H *such that* b *acts quadratically on* V *and such that* b *lies in a subgroup of* G *which is isomorphic to* $SL(2, p)$.

Proof. Suppose false, and let a counter-example (G, V) be chosen with $|G|+|V|$ minimal. As $a \notin O_p(G)$ the Baer–Suzuki theorem implies that there is a conjugate b of a in G such that $\langle a, b\rangle$ is not a p-group. Set $H = \langle a, b\rangle$. Then $a \notin O_p(H)$, and we may therefore assume that a and b are conjugate in H. By minimality of $|G|$ we then have $G = H$.

Suppose first that V is irreducible for G. Then Lemma 2.1 yields $G \cong SL(2, p^n)$ or $SL(2, 5)$, and by minimality we then have $G \cong SL(2, p)$. Moreover, Lemma 2.1 shows also that V is a natural module for G, so we are done in this case. As (G, V) is a counter-example to Lemma 2.4, we conclude that V is reducible. By minimality of $|V|$, all non-central chief factors for G in V are natural $SL(2, p)$-modules for G. Let $W_0 \geqslant W_1 \geqslant W_2$ be a descending chain of G-submodules of V, with irreducible quotients, and set $X = W_0/W_2$ and $\overline{G} = G/C_G(X)$. Suppose that X is indecomposable, and consider first the case in which exactly one of the irreducible constituents for G in X is non-trivial. Then $\overline{G}/O_p(\overline{G})$ is isomorphic to $SL(2, p)$, and $O_p(\overline{G})$ is a natural $SL(2, p)$-module for $\overline{G}/O_p(\overline{G})$. Every element of order p in $\overline{G} - O_p(\overline{G})$ is then contained in a complement to $O_p(\overline{G})$ in $\overline{G}$, and we thereby contradict the minimality of $|G|$. Thus no such indecomposable section X of V exists. It follows that $V = [V, G] \oplus C_V(O^p(G))$, and that both irreducible constituents of X are non-trivial. Let U be the irreducible submodule of X. Then $O_p(\overline{G}) = C_{\overline{G}}(U) = C_{\overline{G}}(X/U)$ as $\overline{G}$ is generated by two conjugate elements of order p, and $\overline{G}/O_p(\overline{G}) \cong SL(2, p)$. Now Lemma 2.3(a) and minimality of $|G|$ together imply that $O_p(\overline{G}) = 1$ and that X is decomposable. We have thus shown that $[V, G]$ is a direct sum of natural $SL(2, p)$-modules for G. □

Lemma 2.5. *Let* $G = K \times \langle c\rangle$, *with* $K \cong SL(2, 5)$ *and with* c *an element of order* 3. *Let* V *be a faithful* $\mathbb{F}_3G$*-module, and suppose that there exists an element* a *of order* 3 *in* G *which acts quadratically on* V. *Then such an element* a *may be chosen to lie in* $K \cup \langle c\rangle$.

Proof. Suppose false, and let b be an element of order 3 in K, with $a \in \langle b, c\rangle$. Also, let L be a subgroup of G, containing a, with $L \cong SL(2, 3)$. Then $[V, K] = [V, Z(K)] = [V, Z(L)] = [V, O_2(L)]$ is a direct sum of natural $SL(2, 3)$-modules for L, by Lemma 2.4(b). As $a \notin K$, c acts quadratically on $C_V(K)$, and then since c is not quadratic on V we conclude that there exists an irreducible L-submodule U of $[V, K]$ such that c is not quadratic on the subspace $W = \langle U^{\langle c\rangle}\rangle$ of V. Then $W = U \oplus U^c \oplus U^{c^2}$, and then also $W = U \oplus U^x \oplus U^{x^2}$ for any $x \in \langle a, c\rangle - \langle a\rangle$. Thus, $\langle a\rangle$ is the unique quadratic subgroup of order 3 in $\langle a, c\rangle$. But $\langle a\rangle = \langle bc\rangle$ or $\langle b^2c\rangle$, where bc and b^2c are conjugate via K. Thus, $\langle a, c\rangle$ contains at least two quadratic subgroups of order 3, and we have a contradiction at this point. □

Lemma 2.6. *Let G be a finite group, p an odd prime, and V a faithful $\mathbb{F}_pG$-module. Suppose that we are given an element a of $G - O_p(G)$ with $[V, a, a] = 0$, and suppose further that G has cyclic Sylow p-subgroups. Let $g \in G - N_G(\langle a\rangle)$, and set $H = \langle a, a^g\rangle$. Then either $H \cong SL(2, p)$ or $p = 3$ and $H \cong SL(2, 5)$.*

Proof. Assume false, and let (G, V) be a counter-example with $|G| + |V|$ minimal. Then V is reducible for the action of H, by Lemma 2.1. As in the proof of Lemma 2.4, let $W_0 \geqslant W_1 \geqslant W_2$ be a properly descending chain of H-submodules of V, set $X = W_0/W_2$, and set $\overline{H} = H/C_H(X)$. Assume that H acts non-trivially on X. As H has cyclic Sylow p-subgroups we then have $O_p(\overline{H}) = 1$. If one of the constituents for H in X is trivial, it then follows that X is completely reducible, and this shows that each irreducible constituent for H in $[V, H]$ is either a natural $SL(2, p)$-module or, exceptionally, a natural $SL(2, 9)$-module for H. Now let U be an irreducible H-submodule of V, chosen if possible so that $[U, H] = 0$, and set $\widehat{H} = H/C_H(U)$. Then $O^p(H)$ acts non-trivially on V/U, and by the minimality of $|V|$ we then have $\widehat{H} \cong SL(2, p)$ or $SL(2, 5)$. Set $K = C_H(V/U)$. Then K is a normal p'-subgroup of H, and $K \neq 1$ as otherwise we are done. Then K acts non-trivially on U, so U is a natural $SL(2, p)$ or $SL(2, 9)$-module for H, and $|K| = 2$. Thus H is a central extension of $SL(2, p)$ or $SL(2, 9)$ by a group of order 2. But for any prime power q, the 2-part of the Schur multiplier of $SL(2, q)$ is trivial, and so H has a direct factor of order 2. This is contrary to H being generated by two elements of order p, and the lemma is thereby proved. □

Lemma 2.7. *Let G be a finite group, p an odd prime, and A a subgroup of G such that $G = \langle A^G\rangle$. Suppose that G has a faithful $\mathbb{F}_p$-module M such that $[M, A, A] = 0$. Then for any element a of A and any conjugate b of a in G, either $\langle a, b\rangle$ is a p-group, or the following hold.*

(a) *$\langle a, b\rangle$ has a normal subgroup N such that $\langle a, b\rangle/N$ is isomorphic to one of the groups $SL(2, p^n)$ $(n \geqslant 1)$, or $SL(2, 5)$.*
(b) *$\langle a, b\rangle$ has a subgroup $K = \langle a^K\rangle$ with K isomorphic to $SL(2, p)$ or $SL(2, p) \times \mathbb{Z}_p$. Moreover, if $p = 3$ then $K \cong SL(2, 3)$.*

Proof. Let $a \in A$ and let $b \in a^G$, and put $L = \langle a, b\rangle$. Suppose that L is not a p-group, and let W be a non-trivial irreducible constituent in M for the action of L. Setting $N = C_L(W)$, it follows from Lemma 2.1 that L/N is isomorphic to $SL(2, p^n)$ for some n, or to $SL(2, 5)$. Further, Lemma 2.4 implies that L has a subgroup $K = \langle a^K\rangle$ with K isomorphic to $SL(2, p)$ or $\mathbb{Z}_p \times SL(2, p)$. □

The following beautiful result is due to Ulrich Meierfrankenfeld.

Lemma 2.8. *Let G be a finite group, p a prime, $p > 3$, and let V be a faithful, irreducible $\mathbb{F}_pG$-module. Suppose that $G = \langle A^G\rangle$, where A is a non-identity subgroup of G which acts quadratically on V. Suppose further that G has cyclic Sylow p-subgroups, and that all involutions in $C_G(A)$ are contained in $Z(G)$. Then $G \cong SL(2, p)$.*

Proof. Let $g \in G - N_G(A)$, set $H = \langle A, A^g \rangle$, and set $B = N_H(A)$. As G has cyclic Sylow p-subgroups, we have $H \cong SL(2, p)$, by Lemma 2.6. The involution z in H is then in $Z(G)$, and since V is irreducible we have $V = [V, z]$. Then Lemma 2.4(b) implies that $V = \bigoplus_{1 \leqslant i \leqslant n} V_i$, where each V_i is a natural $SL(2, p)$-module for H. As $p > 3$, B is non-abelian and we find that $Aut_B(V_i) = Aut_H(V_i)$ for all i. Setting $D = Aut_H(V)$, it follows that $Aut_B(V) = D$.

The centralizer in G of the chain $V \geqslant C_V(A) \geqslant 0$ acts quadratically on V, and is therefore an elementary abelian p-subgroup of G containing A. As G has cyclic Sylow p-subgroups we therefore conclude that

$$A = C_G\big(C_V(A)\big) \cap C_G\big(V/C_V(A)\big). \tag{1}$$

Now let $\widetilde{H}$ be a subgroup of G with $A \leqslant \widetilde{H} \cong H$, and set $\widetilde{B} = N_{\widetilde{H}}(A)$. The image of B in $GL(C_V(A)) \times GL(V/C_V(A))$ is $\{(\lambda I, \lambda^{-1} I)\colon\ 0 \neq \lambda \in \mathbb{F}_p\}$, and the same is true of $\widetilde{B}$. Then (1) implies that $B = \widetilde{B}$, and so $Aut_{\widetilde{H}}(V) = Aut_{\widetilde{B}}(V) = D$. On the other hand, we have $Aut_D(V) \cong GL(2, p)$, and $\langle H, \widetilde{H} \rangle \leqslant Aut_D(V)$. Thus $H = \widetilde{H}$.

For any $x \in G - N_G(A)$, we may now conclude that $\langle A^x, A^{gx} \rangle = \langle A, A^x \rangle$ (by replacing A by A^x in the preceding discussion). Since also $H = \langle A, A^g \rangle = \langle A, A^x \rangle$, we conclude that H is invariant under $\langle G - N_G(A) \rangle$. That is, H is G-invariant, and thus $H = \langle A^G \rangle = G$. □

Lemma 2.9. *Assume Hypothesis* 1.1, *and let a be a non-identity element of A. Suppose that we are given a p'-subgroup Q of G, with $[Q, a] = Q$. Then $p = 3$ and Q is a non-abelian* 2*-group. Moreover, if Q is extraspecial then Q is a quaternion group.*

Proof. Let R be an a-invariant Sylow subgroup of Q, with $[R, a] \neq 1$. Then Lemma 2.7(b) implies that $p = 3$, R is a 2-group, and $Q = C_Q(a)R$. But then also $Q = R$, since $Q = [Q, a]$. Further, Lemma 2.7(b) also shows that every a-invariant abelian subgroup of Q is centralized by a, and so Q itself is non-abelian. Now suppose that Q is extraspecial. Then $C_Q(a) = Z(Q)$, and it follows that for any involution t in $Q - Z(Q)$ we have $\langle t, a \rangle$ containing a subgroup isomorphic to $Alt(4)$. Therefore there is no such involution t, and so Q is a quaternion group. □

Lemma 2.10. *Assume Hypothesis* 1.1, *let $a \in A$, and let L be an a-invariant subgroup of G. Then every component of L is a-invariant.*

Proof. Suppose false, and let K be a component of L which is not a-invariant. As K is quasisimple, there is a prime divisor r of $|K/Z(K)|$ with $r \notin \{2, p\}$. Let R be a Sylow R-subgroup of K. Then $[R, a]$ is a non-identity r-group, and we contradict Lemma 2.9. □

3. Groups of Lie type

In this section we collect the information that we need concerning automorphisms, Schur multipliers, and centralizers of semisimple elements in groups of Lie type. In doing

so, we are guided to a great extent by [6]. Many of the results from [6] that we quote come indirectly from [13–15], and [7].

Let r be a prime, let $\overline{F}$ be an algebraic closure of the field $\mathbb{F}_r$ of r elements, and let $\overline{K}$ be a simple (linear) algebraic group defined over $\overline{F}$. (If also $Z(\overline{K}) = 1$ then we say that $\overline{K}$ is of *adjoint type*.)

Fix a maximal torus $\overline{T}$ of $\overline{K}$, and let Σ be the root system associated with $\overline{T}$. For any α in Σ, let $\overline{X}_\alpha = \{x_\alpha(t)\colon\ t \in \overline{F}\}$ be the one-parameter subgroup (i.e., the *root subgroup*) of $\overline{K}$ associated with α, and denote by $\mathcal{X}$ the set of all elements $x_\alpha(t)$ of $\overline{K}$, $\alpha \in \Sigma$ and $t \in \overline{F}$. The root subgroups of $\overline{K}$ generate $\overline{K}$, so any endomorphism of $\overline{K}$ is determined by its action on $\mathcal{X}$.

A surjective algebraic endomorphism σ of $\overline{K}$ is said to be a *Steinberg endomorphism* if $C_{\overline{K}}(\sigma)$ is finite. A finite group K is a *group of Lie type* (*in characteristic* r) if $K = O^{r'}(C_{\overline{K}}(\sigma))$ for some simple algebraic group $\overline{K}$ and some Steinberg endomorphism σ of $\overline{K}$. Following [6], we then say that $(\overline{K}, \sigma)$ is a σ*-setup* of K. If $\overline{K}$ is of adjoint type (i.e., if $Z(\overline{K}) = 1$) then $Z(K) = 1$, and we say also that K is of *adjoint type*. The class of groups of Lie type in characteristic r is denoted $Lie(r)$.

Let $q = r^n$ be a power of r, where n is a positive integer. There is then a Steinberg endomorphism ϕ_q of $\overline{K}$ given on $\mathcal{X}$ by

$$\phi_q\big(x_\alpha(t)\big) = x_\alpha\big(t^q\big). \tag{3.1}$$

For any isometry ρ of Σ there is an automorphism γ_ρ of $\overline{K}$ given on $\mathcal{X}$ by

$$\gamma_\rho\big(x_\alpha(t)\big) = x_{\alpha^\rho}(t). \tag{3.2}$$

If Σ is B_2, F_4, or G_2, and r is 2, 2, or 3, respectively, then there is a unique angle-preserving, length-changing bijection ρ on Σ, and there is an automorphism ψ of $\overline{K}$ given on $\mathcal{X}$ by

$$\psi\big(x_\alpha(t)\big) = \begin{cases} x_{\alpha^\rho}(t) & \text{if } \alpha \text{ is long,} \\ x_{\alpha^\rho}(t^r) & \text{if } \alpha \text{ is short.} \end{cases} \tag{3.3}$$

One observes that ϕ_r commutes with γ_ρ for any isometry ρ of Σ, and in the special cases given by (3.3) one observes that $\psi^2 = \phi_r$.

The following result is Theorem 2.2.3 in [6].

Proposition 3.4. *Let $K \in Lie(r)$ and let $(\overline{K}, \sigma)$ be a σ-setup of K. Then there is a maximal torus $\overline{T}$ of $\overline{K}$, with associated root system Σ, such that, after conjugating σ by a suitable inner automorphism of $\overline{K}$, one of the following holds.*

(i) *$\sigma = \gamma_\rho \circ \phi_q$ for some isometry ρ of Σ and some positive integral power q of r.*
(ii) *$\Sigma = B_2$, F_4, or G_2, with $r = 2$, 2, or 3, respectively, and $\sigma = \psi^n$ for some odd positive integer n, where ψ is as in* (3.3).

The group K in Proposition 3.4 may be denoted ${}^d\Sigma(q)$, where $d = |\rho|$ in case (i), and where $d = 2$ in case (ii). If $d = 1$ then we may write simply $K = \Sigma(q)$, and we say in this case that K is a *Chevalley group*. If $d \neq 1$ and σ is conjugate to $\gamma_\rho \circ \phi_q$, where ρ is a non-trivial isometry of Σ, then K is a *Steinberg variation*. If $d = 2$ and σ is conjugate to ψ^n, n odd, where ψ is as in (3.3), then K is a *Ree–Suzuki group*.

Let $K = {}^d\Sigma(r^n) \in Lie(r)$, let $(\overline{K}, \sigma)$ be a σ-setup of K, and let x be an automorphism of K. We say that x is an *inner-diagonal automorphism* if x is the restriction to K of an inner automorphism of $C_{\overline{K}}(\sigma)$. The group of all inner-diagonal automorphisms of K is denoted $Inndiag(K)$. We say that x is a *field automorphism* if x is conjugate via $Inndiag(K)$ to a non-identity automorphism of the form $\phi_q|_K$. We say that x is a *graph automorphism* if $d = 1$ and x is conjugate via $Inndiag(K)$ to an automorphism of the form $(\gamma_\rho)|_K$, ρ a non-identity isometry of Σ. We say that x is a *graph-field automorphism* if either $d = 1$ and x is conjugate via $Inndiag(K)$ to an automorphism of the form $(\gamma_\rho \circ \phi_q)|_K$ of $\overline{K}$, ρ a non-trivial isometry of Σ, or if $d = 2$ and x is conjugate via $Inndiag(K)$ to an automorphism of the form ψ^n, n odd, where ψ is given as in (3.3).

If Σ is not B_2, F_4, or G_2, with $p = 2, 2$, or 3, respectively, set $\psi = \phi_r$. In any case, set $\Phi_{\overline{K}} = \langle\psi\rangle$. Also, denote by $\Gamma_{\overline{K}}$ the set of all γ_ρ, ρ an isometry of Σ.

Proposition 3.5. *Let K be a group of Lie type and let $(\overline{K}, \sigma)$ be a σ-setup for K. Assume that $Z(\overline{K}) = 1$, and identify $\overline{K}$ with the group of inner automorphisms of $\overline{K}$. Denote by $Aut_1(\overline{K})$ the group of automorphisms τ of $\overline{K}$ as an abstract group, such that either τ or τ^{-1} is an algebraic endomorphism of $\overline{K}$. Then the following hold.*

(a) *We have $Aut_1(\overline{K}) = (\Phi_{\overline{K}} \times \Gamma_{\overline{K}})\overline{K}$.*
(b) *The restriction map from $C_{Aut_1(\overline{K})}(\sigma)$ to $Aut(K)$ is surjective, with kernel $\langle\sigma\rangle$.*
(c) *We have $C_{Aut_1(\overline{K})}(K) = \langle\sigma\rangle$.*

Proof. Parts (b) and (c) are Theorem 2.5.4 and Lemma 2.5.7, respectively, in [6]. Part (a) follows from (b) and from the theorem of Steinberg [13, Theorem 30] which states that every automorphism of K is the product of inner-diagonal, field, and graph automorphisms. □

The next result is [6, Proposition 4.9.1]. The proof given below is essentially the same as in the cited reference.

Proposition 3.6. *Let $K = {}^d\Sigma(q) \in Lie(r)$, with $Z(K) = 1$. Let x be a field automorphism or a graph-field automorphism of K, of prime order p, and let $y \in Inndiag(K)x$. If K is a Steinberg variation, assume that $d \neq p$. Then x and y are conjugate via $Inndiag(K)$.*

Proof. Let $(\overline{K}, \sigma)$ be a σ-setup of K, with $Z(\overline{K}) = 1$. If K is a Chevalley group or a Ree–Suzuki group (resp. a Steinberg variation) we may take $\sigma = \psi^n$ (resp. $\gamma_\rho \circ \phi_{r^n}$ for some appropriate $n > 0$). We claim:

There exists a Steinberg endomorphism τ of $\overline{K}$, with $x \in \langle\tau|_K\rangle$ and with $\tau^p = \sigma$. (1)

Suppose that (1) holds, and let k be the integer, $1 \leqslant k < p$, such that $\tau|_K = x^k$. We are given $y \in Aut(K)$ with $y \in Inndiag(K)x$. Identify $Inndiag(K)$ with $C_{\overline{K}}(\sigma)$. Then y^k is the restriction to K of some automorphism $\tau_1 = h\tau$ of $\overline{K}$, where $h \in C_{\overline{K}}(\sigma)$. As $|y^k| = p$, we have $(\tau_1)^p \in \langle\sigma\rangle$, by Proposition 3.5(c). As $\tau_1^p \equiv \tau^p \pmod{Inndiag(K)}$, we then have $\tau_1^p = \sigma$, by (1). As τ is a Steinberg endomorphism of $\overline{K}$ we may apply Lang's Theorem [6, Theorem 2.1.1]), and conclude that $h = g\tau g^{-1}\tau^{-1}$ for some $g \in \overline{K}$. Then $\tau_1 = g\tau g^{-1}$, and by taking pth powers we obtain $\sigma = g\sigma g^{-1}$. Thus $g \in C_{\overline{K}}(\sigma) = Inndiag(K)$, and $y = gxg^{-1}$, as required. Thus, it remains to establish (1).

Set $\Phi = \Phi_{\overline{K}}$ and $\Gamma = \Gamma_{\overline{K}}$. By Proposition 3.4, we may take $\sigma = \psi^n \circ \gamma_\rho$ for some $n > 0$ and some isometry ρ of Σ. We are free to replace x by any $Inndiag(K)$-conjugate of x, and then since x is a field or graph-field automorphism of K we may take $x = \tau_0|_K$, for some $\tau_0 \in \Phi\Gamma$. Moreover, we have $[\sigma, \tau_0] = 1$ by Proposition 3.5(b), and $(\tau_0)^p \in \langle\sigma\rangle$ by Proposition 3.5(c).

Suppose that $\tau_0 \in \Gamma\langle\sigma\rangle$. By assumption, x is not a graph automorphism of K, so K is not a Chevalley group. If K is a Ree–Suzuki group then $\Gamma = 1$, and since $\tau_0 \notin \langle\sigma\rangle$ we conclude that K is a Steinberg variation. Then $\rho \neq 1$, and since τ_0 and σ commute it follows that $\tau_0 \in \langle\rho, \sigma\rangle$. Then $d = p$, contrary to assumption. Thus, we conclude that $\tau_0 \notin \Gamma\langle\sigma\rangle$.

We have $\Phi\Gamma/\langle\sigma\rangle\Gamma \cong \mathbb{Z}_n$, and since $x^p = 1$ it now follows that p divides n. Write $n = pm$ and set $\psi_1 = \psi^m$. Suppose that $\rho = 1$. We then have $(\psi_1)^p = \sigma$, and $\tau_0 \in \langle\psi_1\rangle\Gamma$. Write $\tau_0 = (\psi_1)^k\gamma$, where $\gamma \in \Gamma$. As $[\Phi, \Gamma] = 1$ we conclude that $|\gamma| = 1$ or p, so there exists an integer ℓ with $\gamma^{k\ell} = \gamma$. We then take $\tau = \psi_1\gamma^\ell$, and obtain $\tau^p = \sigma$ and $\tau^k = \tau_0$. Thus, (1) holds in this case. On the other hand, suppose that $\rho \neq 1$. Then p does not divide $|\rho|$, by assumption, and so there exists $\gamma \in \langle\gamma_\rho\rangle$ with $\gamma^p = \rho$. Setting $\tau = \psi_1\gamma$, we then have $\tau^p = \sigma$. Any homomorphic image of $\Phi \times \langle\gamma_\rho\rangle$ has at most one subgroup of order p, so $x \in \langle\tau|K\rangle$, and thus (1) holds in any case. □

We next consider centralizers of semisimple elements.

Lemma 3.7. *Let K be a simple group of Lie type in characteristic r, and let $(\overline{K}, \sigma)$ be a σ-setup of K. Identify $Inndiag(K)$ with $C_{\overline{K}}(\sigma)$, and let $x \in Inndiag(K)$ with $|x|$ prime to r. Then the following conditions are equivalent.*

(1) *$C_{\overline{K}}(x)$ contains a non-identity unipotent element.*
(2) *$O^{r'}(C_K(x)) \neq 1$.*
(3) *$O^{r'}(C_K(x))$ is a product $L_1 \cdots L_n$ $(n \geqslant 1)$, where each L_i is a group of Lie type in characteristic r, and where $[L_i, L_j] = 1$ for all i and j with $i \neq j$.*

Proof. Set $\overline{C} = C_{\overline{K}}(x)$. As $|x|$ is relatively prime to r, x is a semisimple element of $\overline{K}$, and hence $\overline{C}$ is closed and reductive. Set $\overline{L} = [\overline{C}, \overline{C}]$. Thus $\overline{C} = Z(\overline{C})\overline{L}$, where $\overline{L}$ is closed and semisimple, and where $Z(\overline{C})$ is a torus. Then $\overline{L}$ contains all of the unipotent elements of $\overline{C}$. Denote by $\mathcal{M}$ the set of normal, simple algebraic subgroups of $\overline{L}$. Then $\overline{L}$ is the commuting product of the members of $\mathcal{M}$. If $\mathcal{M}$ is non-empty, we write $\mathcal{M} = \{\overline{M}_i\}_{1 \leqslant i \leqslant t}$. Notice that

if $L = 1$ then $C_K(x) = C_{\overline{C}}(\sigma)$ consists of semisimple elements, so that $O^{r'}(C_K(x)) = 1$. Thus (2) implies (1).

Suppose that $\mathcal{M}$ is non-empty. That is, assume that (1) holds. As σ commutes with x, $\overline{C}$ is σ-invariant and σ then induces a permutation action on $\mathcal{M}$. Let $\mathcal{M}_1, \ldots, \mathcal{M}_n$ be the orbits for σ on $\mathcal{M}$, and assume (without loss) that indices have been chosen so that $\mathcal{M}_1 = \{\overline{M}_i\}_{1 \leqslant i \leqslant k}$. Since any positive power of a Steinberg endomorphism is again a Steinberg endomorphism, it follows that σ^k induces a Steinberg endomorphism on each $\overline{M}_i$, $1 \leqslant i \leqslant k$. For such i, set $M_i = O^{r'}(C_{\overline{M}_i}(\sigma^k))$. Then each M_i is a group of Lie type in characteristic r, by definition. Now set $M = M_1 \cdots M_k$. Then $M/Z(M)$ is the direct product of the images in $M/Z(M)$ of the groups M_i, $1 \leqslant i \leqslant k$, and the action of σ on $M/Z(M)$ is given by the transitive permuting of these factors. Set $L_1 = O^{r'}(C_{\overline{M}}(\sigma))$. It now follows that L_1 is isomorphic to a quotient of M_1 by a subgroup of $Z(M_1)$. We repeat this procedure for the remaining σ-orbits, obtaining the groups L_1 through L_n.

Now set $L = O^{r'}(C_{\overline{L}}(\sigma))$. Since central quotients of groups in $Lie(r)$ are also in $Lie(r)$, we conclude that L is the pairwise commuting product of the groups L_j, $1 \leqslant j \leqslant n$, where each L_j is a member of $Lie(r)$. On the other hand, we have $C_{\overline{K}}(\sigma) = C_{\overline{T}}(\sigma)K$ for some σ-invariant maximal torus $\overline{T}$, and then

$$L = O^{r'}\big(C_{\overline{K}}\big(\langle \sigma, x\rangle\big)\big) = O^{r'}\big(C_{C_{\overline{K}}(\sigma)}(x)\big) = O^{r'}\big(C_K(x)\big).$$

Thus (3) holds. Clearly, (3) implies (2), and thus the lemma is proved. □

Lemma 3.8. *Let r be a prime and let $\overline{K}$ be a simple linear algebraic group over an algebraic closure $\overline{F}$ of the field $F = \mathbb{F}_r$ of r elements. Let σ be a Steinberg endomorphism of $\overline{K}$, and set $K = O^{r'}(C_{\overline{K}}(\sigma))$ (so that K is a group of Lie type in characteristic r). Let $g \in K$, and assume that either*

(i) $|g| = 2$ *and $\overline{K}$ is not of type A_1, or*
(ii) $|g| = 3$ *and $\overline{K}$ is not of type A_1 or A_2.*

Then $C_{\overline{K}}(g)$ contains a non-identity unipotent element.

Proof. We may assume that $|g| \neq r$ as otherwise the result holds trivially. Thus g is a semisimple element of $\overline{K}$, and so there is a maximal torus $\overline{T}$ of $\overline{K}$ containing g. Let Σ be the root system for $\overline{K}$ given by $\overline{T}$, Π a fundamental system in Σ, $\overline{B}$ the corresponding Borel subgroup, and $\overline{U}$ the unipotent radical of $\overline{B}$. Recall that each $\alpha \in \Sigma$ is a homomorphism of $\overline{T}$ into $\overline{F}^\times$, and that there is then a $\overline{T}$-invariant subgroup $\overline{U}_\alpha$ of $\overline{U}$ and a parametrization

$$x_\alpha : \overline{F}^\times \to \overline{U}_\alpha$$

such that $g x_\alpha(t) g^{-1} = x_\alpha(\alpha(g)t)$ for all $t \in \overline{F}^\times$.

We aim to show that, under the conditions given in (i) and (ii), there exists a root α such that $\overline{U}_\alpha \leqslant C_{\overline{K}}(g)$. Suppose false, and suppose first that $|g| = 2$. Here $\alpha(g)^2 = 1$, so we have $\alpha(g) = -1$ for all $\alpha \in \Sigma$. Assuming that Σ is not A_1, there exist two roots α and β

whose sum is a root, and we then have $(\alpha+\beta)(g)=\alpha(g)\beta(g)=1$, for a contradiction. Now suppose that $|g|=3$, and let ω be a primitive cube root of unity in $\overline{F}$. Then $\alpha(g)=\omega$ or ω^{-1} for all roots α. It follows that $\alpha(g)=\beta(g)\neq 1$ whenever α and β are roots whose sum is again a root. In particular, we may assume that $\alpha(g)=\omega$ for all $\alpha\in\Pi$. If Σ has more than one root length then there are fundamental roots α and β such that $\alpha+2\beta$ is a root, and we obtain $(\alpha+2\beta)(g)=1$ in that case. Also, if the rank of Σ is at least 3 then there exist fundamental roots α, β, and γ whose sum is a root, yielding $(\alpha+\beta+\gamma)(g)=1$. Thus, Σ is of rank at most two, and Σ has only one root length. That is, Σ is A_1 or A_2. □

Lemma 3.9. *Let K be a simple group of Lie type in characteristic r, let p be a prime different from r, and let x be an element of order p in Inndiag(K). Suppose that x is contained in a non-cyclic abelian p-subgroup of Inndiag(K). Then there exists an element y of order p in $C_K(x)$ such that $O^{r'}(C_K(y))\neq 1$.*

Proof. Let E be an elementary abelian subgroup of *Inndiag*(K) of order p^2, containing x, and let $(\overline{K},\sigma)$ be a σ-setup for K. Let $\overline{T}$ be a maximal torus of $\overline{K}$ containing E, let $\overline{B}$ be a Borel subgroup of $\overline{K}$ containing $\overline{T}$, let Σ be the root system defined by $\overline{T}$ and $\overline{B}$, and let $\alpha\in\Sigma$. Then α is a homomorphism of $\overline{T}$ into the multiplicative group of an algebraic closure of $\mathbb{F}_r$. The image of α is then cyclic, and so there exists a non-identity element $y\in E\cap \mathrm{Ker}(\alpha)$. This means that $C_{\overline{K}}(y)$ contains the root subgroup of $\overline{B}$ corresponding to α. The desired result then follows from Lemma 3.7. □

We next consider normalizers of r-groups in groups K, $K\in Lie(r)$.

Lemma 3.10 (Borel–Tits). *Let $K\in Lie(r)$ and let R be a non-identity r-subgroup of K. Then there is a parabolic subgroup P of K such that $R\leqslant O_r(P)$ and $N_K(R)\leqslant P$.*

Proof. This result, proved first in [2], appears as [6, Theorem 3.1.3(a)]. □

Recall that a group G is said to be *r-constrained* if $C_G(O_r(G))\leqslant O_r(G)$.

Lemma 3.11. *Let $K\in Lie(r)$, let X be a subgroup of Aut(K) containing Inn(K), and let R be a non-identity r-subgroup of K. Then the following hold.*

(a) *Both $C_X(R)$ and $N_X(R)$ are r-constrained.*
(b) *If $R=O_r(N_K(R))$ then the group $P=N_K(R)$ is a parabolic subgroup of K, and $R=O_r(P)$.*

Proof. See [6, Corollaries 3.1.4 and 3.1.5]. □

We now review the Schur multipliers of the groups of Lie type.

Proposition 3.12. *Let K be a simple group of Lie type, in characteristic r, and let $\widehat{K}$ be the universal, perfect central extension of K. Set $Z=Z(K)$. Then $Z=Z_c\times Z_e$, where Z_c (the "canonical" part of Z) is isomorphic to the quotient group Outdiag$(K)=$*

Inndiag$(K)/Inn(K)$, *and where* Z_e (*the "exceptional" part of* Z) *is equal to* $O_r(Z)$. *Moreover, we have* $Z_e = 1$ *except in the following cases.*

(a) $|Z_e| = 2$, *and* K *is isomorphic to* $L_2(4)$, $L_3(2)$, $Sp(4,2)'$, $L_4(2)$, $Sp(6,2)$, $U_4(2)$, $F_4(2)$, *or* $G_2(4)$.
(b) $Z_e \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, *and* K *is isomorphic to* $U_6(2)$, $D_4(2)$, $Sz(8)$, *or* ${}^2E_6(2)$.
(c) $Z_e \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, *and* K *is isomorphic to* $L_3(4)$.
(d) $|Z_e| = 3$, *and* K *is isomorphic to* $L_2(9)$, $\Omega_7(3)$, *or* $G_2(3)$.
(e) $Z_e \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, *and* K *is isomorphic to* $U_4(3)$.

Proof. The relevant references are [15], and [7]. See also Chapter 6 of [6]. □

Lemma 3.13. *Let* G *be a finite group, put* $X = O_2(G)$, *and assume that* $X = F^*(G)$ *is an extraspecial* 2*-group of width* n *and sign* ε. *Assume also that either*:

(1) $G/X \cong \Omega^{\varepsilon}_{2n}(2)$ *with* $n \geqslant 3$ *if* $\varepsilon = 1$, *or*
(2) $G/X \cong SU(n,2)$ *with* $n \neq 2$, *and with* $\varepsilon = (-1)^n$.

Let G^* *be a group having a normal subgroup* $\langle t\rangle$ *of order* 2, *with* $G^*/\langle t\rangle \cong G$. *Then* $O_2(G^*) \cong X \times \langle t\rangle$.

Proof. Put $M = X/Z(X)$. Then the squaring map from M into $Z(X)$ defines a quadratic form Q on M, with respect to which M is a non-degenerate orthogonal space over $\mathbb{F}_2$, of sign ε. If $G/X \cong \Omega^{\varepsilon}_{2n}(2)$, it follows that M may be identified with the natural G/X-module. If $G/X \cong SU(n,2)$, then M may be identified with the natural n-dimensional hermitian module for G/X over $\mathbb{F}_4$, whose hermitian form h satisfies $h(v,v) = Q(v)$ for all $v \in M$. In both the cases (1) and (2), the singular vectors and the non-singular vectors in M with respect to Q each form a single orbit for the action of G/X.

Denote by Z the pre-image of $Z(X)$ in G^*. Also, denote by $\mathcal{D}$ the set of subgroups D of G such that $[X,D] = [X,D,D]$ is a quaternion group. Thus, $\mathcal{D}$ is a set of groups of order 3, and since $n \geqslant 3$ if $G/X \cong \Omega^+(2n,2)$ it follows that $\mathcal{D}$ is non-empty. Fix $D \in \mathcal{D}$, and denote by Y the inverse image of $\langle D^X\rangle$ in G^*. Then Y is isomorphic to $SL(2,3) \times \mathbb{Z}_2$. Denote by z the involution in $Z(Y)$, set $G_0^* = C_{G^*}(z)$, and let G_0 be the image of G_0^* in G. Then $|G : G_0| \leqslant 2$, and $z \neq t$. We now make the following claim.

For any element x^* of $O_2(G^*)$ whose image in G has order 4, we have $(x^*)^2 = z$. $(*)$

Suppose that $(*)$ is not the case. As G is transitive on the non-singular vectors in M, it follows that $G \neq G_0$, and that G_0 has two orbits on $\mathcal{D}$. Let $\mathcal{D}_0$ and $\mathcal{D}_1$ be the two orbits for G_0 on $\mathcal{D}$. Then, for any $D_0 \in \mathcal{D}_0$ and any $D_1 \in \mathcal{D}_1$, we have $|[X,D_0] \cap [X,D_1]| = 2$, and hence $[X,D_0]$ commutes with $[X,D_1]$. Thus $[X,\langle\mathcal{D}_0\rangle]$ commutes with $[X,\langle\mathcal{D}_1\rangle]$, and so each $[X,\langle\mathcal{D}_i\rangle]$ is a proper subgroup of X. In particular, it follows that $\langle\mathcal{D}_i\rangle \neq O^2(G)$, and hence $G/X \cong \Omega_4^+(2)$ or $SU(2,2)$. These two cases are excluded by the conditions placed on n in (1) and (2), so $(*)$ holds.

Now let $s \in X$ be an involution. By transitivity of G/X on singular points, we may assume that Y was chosen so that $\langle D^X, s\rangle \cong SL(2,3) \circ \mathbb{Z}_4$ (the central product). Denote by L the pre-image of $\langle D^X, s\rangle$ in G^*. Then $O_2(L)$ is not isomorphic to $Q_8 \times \mathbb{Z}_4$, by $(*)$, and therefore s lifts to an involution in G^*. This shows that $\{g^2\colon\ g \in O_2(G^*)\}$ is of cardinality 2, and hence $|\Phi(O_2(G^*))| = 2$. This yields the lemma. □

Lemma 3.14. *Let K be one of the groups $Sz(8)$, $L_3(4)$, $D_4(2)$, or $U_6(2)$, and let α be an outer automorphism of K of order* 3. *Define $\widehat{K}$ and Z_e as in Proposition* 3.12. *Then α lifts to an automorphism of $\widehat{K}$ which acts faithfully on Z_e.*

Proof. The result is contained in [6, Theorem 6.3.1], but we present an alternative proof here.

Assume that α acts trivially on $Z(\widehat{K})$, let K_1 be a perfect central extension of K by $\mathbb{Z}_2$, and view α as an automorphism of K_1. Suppose first that $K \cong L_3(4)$. Let P be an α-invariant maximal parabolic subgroup of K. Then P is a semidirect product of $SL(2,4)$ with the natural $SL(2,4)$-module, and α centralizes a complement to $O_2(P)$ in P. Let P_1 denote the pre-image of P in K_1. Then $O_2(P_1)$ is elementary abelian, since P acts transitively on the non-identity elements of $O_2(P)$. Further, we may choose K_1 so that P_1 has a subgroup isomorphic to $SL(2,4)$, since $SL(2,4)$ has no perfect central extension by $\mathbb{Z}_2 \times \mathbb{Z}_2$. But now $[O_2(P_1), \alpha](C_{P_1}(\alpha))'$ is isomorphic to P, and is a complement to $Z(K_1)$ in P_1. Gaschütz's Theorem [1, result (10.4)] then implies that K_1 splits over $Z(K_1)$, and we have a contradiction.

Suppose next that $K \cong U_6(2)$. Then $K\langle\alpha\rangle$ has a subgroup P of the form $2_+^{1+8} : (U_4(2) \times 3)$. The Schur multiplier of $U_4(2)$ contains no fours group, so there is a perfect central extension of $K\langle\alpha\rangle$ by $\mathbb{Z}_2$ in which P lifts to a group P_1 having a subgroup $U_4(2) \times 3$. By Lemma 3.13, $O_2(P_1)$ splits over $Z(K_1)$, and as in the case of $L_3(4)$ we find that $[O_2(P_1), \alpha](C_{P_1}(\alpha))'$ is a complement to $Z(K_1)$ in P_1, and a contradiction is reached as before.

Suppose that $K \cong Sz(8)$. Let S be an α-invariant Sylow 2-subgroup of K and put $U = \Omega_1(S)$. Then $U = Z(S)$, and $N_K(S)$ acts transitively on the set of non-identity elements of U. Let S_1 and U_1 denote the pre-images of S and U, respectively, in K_1. It follows at once that U_1 is elementary abelian. We have $C_S(\alpha) \cong \mathbb{Z}_4$, and since all involutions in S_1 lie in U_1 it then follows that $C_{S_1}(\alpha) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. Let $u \in C_{U_1}(\alpha)$ with $u \notin Z(K_1)$. Then $C_{S_1}(u)$ is α-invariant, of index at most 2 in S_1, and containing $C_{S_1}(\alpha)$. We conclude that in fact $u \in Z(S_1)$, and hence $U_1 = Z(S_1)$. Now let U^* and S^* be the inverse images of U and S in the full covering group K^* of K, and let X be a subgroup of $N_{K^*}(S^*)$ of order 7. It follows from the fore-going that $U^* = Z(S^*)$. Let $g \in S^* - U^*$. Then $g^2 = yz$ where $y \in [U^*, X]$ and where $z \in Z(K^*)$. Without loss, we may assume that K_1 was chosen to begin with so that z projects to the identity element of K_1. Taking g_1 for the image of g, and X_1 for the image of X in K_1, we then have $(g_1)^2 \in [U_1, X_1]$, and then $\Phi(S_1) = [U_1, X_1]$. Thus S_1 splits over $Z(K_1)$, with a contradiction as before.

Suppose that $K \cong D_4(2)$. In order to analyze this group we will require the detailed structure of the group $P = V : L$, where $L \cong Alt(8)$ and where $V \cong 2^6$ is the unique non-trivial constituent in the permutation module for L over $\mathbb{F}_2$. Here V may be described as follows. Put $\Omega = \{1, 2, \ldots, 8\}$ and let $\mathcal{E}$ be the $\mathbb{F}_2$-space of all even-cardinality subsets

of Ω, with addition given by symmetric difference. We may then identify V with $\mathcal{E}/\langle\Omega\rangle$, with natural action by L. We require the following facts.

(1) P is isomorphic to a maximal parabolic subgroup of $D_4(2)$.
(2) $L \cong \Omega_6^+(2)$ and V is isomorphic to the natural orthogonal module for L. Moreover, the singular vectors correspond to the four-element subsets of Ω.
(3) We have $H^1(L, V) \cong \mathbb{Z}_2$. (Up to isomorphism, $\mathcal{E}$ is the unique indecomposable L-module of order 2^7 with quotient module V.)

The next two results are easily computed from the above information.

(4) Let S be a Sylow 2-subgroup of P. Then S has exactly three elementary abelian subgroups of order 2^6. They are V, A_1, and A_2, where $|A_i \cap V| = |A_i \cap L| = 8$, and $N_L(A_i \cap L) \cong 2^3 : L_3(2)$.
(5) In the semidirect product $\mathcal{E} : L$, the pre-image of each A_i is an extraspecial group.

From the D_4 diagram, and from (4), we obtain the following fact.

(6) Identify S with an α-invariant Sylow 2-subgroup of K, and P with a maximal parabolic subgroup of K. Then α permutes $\{V, A_1, A_2\}$ transitively.

With these facts in hand, one may prove that α acts non-trivially on the Schur multiplier of K. For, taking K_1 as in the previous cases, suppose first that V lifts in K_1 to a group V_1 which is elementary abelian. Then (4) and (6) imply that the pre-image L_1 of L is isomorphic to $L \times \mathbb{Z}_2$. The inverse image P_1 of P is then isomorphic to $\mathcal{E} : L$, as otherwise $Z(K_1)$ has a complement in P. Now (4) and (5) imply that the generalized Fitting subgroups of the pre-images in K_1 of the remaining two connected maximal parabolics over S are extraspecial. Since α fuses these to V_1, we have a contradiction. We therefore conclude that V_1 is not abelian, and so V_1 is extraspecial. In the four-fold covering group $\widehat{K}$ the pre-image V^* of V is then of the form $2_+^{1+6} \times 2$, by Lemma 3.13. But then, taking $\widehat{K}/(V^*)'$ in place of K_1, we have a perfect double cover of K in which the pre-image of V is abelian, after all, and so we have a contradiction at this point. □

4. Automorphisms and alternating groups

Our aim in this section is to prove the following result.

Proposition 4.1. *Let G be a minimal counterexample to Theorem* A. *Then either $\overline{H}$ is a sporadic group, or $\overline{H} \in Lie(r)$, $r \neq p$, and A induces a group of inner-diagonal automorphisms of $\overline{H}$.*

Lemma 4.2. *Assume Hypothesis* 1.1, *set $\overline{G} = G/Z(G)$, and assume that $\overline{H}$ is a group of Lie type in characteristic r, possibly with $r = p$. Assume further that G is a minimal*

counter-example to Theorem A*, and let* $a \in A$*. Then* a *induces an inner-diagonal automorphism of* $\overline{H}$*.*

Proof. Denote by α the automorphism of $\overline{H}$ induced by a. By Proposition 3.5 we have $\alpha = xfg$ where x is an inner-diagonal automorphism, and where f and g are field and graph automorphisms, respectively. We assume that $\alpha \neq x$, and our aim will be to derive a contradiction from this assumption. We proceed by induction on $|G|$.

Suppose first that $\bar{a}$ is not contained in any r-local subgroup of $\overline{G}$. Then $r \neq p$, and α is not conjugate to f in $Aut(\overline{H})$. Then Proposition 3.6 implies that $p = 3$, and that $\overline{H} \cong D_4(q)$ or ${}^3D_4(q)$ for some power q of r. As a is contained in an $SL(2, 3)$ subgroup of G, $\bar{a}$ is in a 2-local subgroup of $\overline{G}$, and so $r \neq 2$. Let b be an element of order 3 in $C_H(a)$, and set $L = O^{r'}(C_H(b))$. Then Lemmas 3.8 and 3.7 together imply that $L \neq 1$ and that $L = L_1 \cdots L_k$ is a commuting product of groups $L_i \in Lie(r)$. Moreover, as $r > 3$, each L_i is quasisimple. If $k \geqslant 3$ and a permutes the factors L_1, L_2, and L_3, then L contains an abelian $3'$-subgroup on which a acts non-trivially, and contrary to Lemma 2.9. Thus, a fixes each of the factors L_i. If $[L_1, a] = 1$ then a is in an r-local subgroup, so in fact $[L_1, a] \neq 1$. We note that $L_1 \neq H$ since $O_3(G) = 1$. By the induction hypothesis, a induces an inner-diagonal automorphism on L_1, and then since $r \neq 2$, induction in Theorem A implies that $r = 5$ and $L_1 \cong SL(2, 5)$. Now Lemma 2.5 shows that either L_1 or $C_{L_1\langle a\rangle}(L_1)$ contains a quadratic element of order 3. As neither $D_4(q)$ nor ${}^3D_4(q)$ occur as outcomes in Theorem A, we conclude, by induction, that $C_{L_1\langle a\rangle}(L_1)$ contains a quadratic element a_1 of order 3. Now a_1 lies in an r-local subgroup of G, and we may replace a by a_1. That is, we may assume from the beginning, and without loss of generality, that a is in an r-local subgroup of G. As r-local subgroups of $\overline{G}$ are r-constrained, by Lemmas 3.11, 2.9 implies that $r = p$, or $r = 2$ and $p = 3$.

Write $\overline{H} = {}^d\Sigma(q)$ as in Section 3, and suppose first that $r = p$. As $O_p(G) = 1$, Proposition 3.12 implies that $H \in Lie(r)$, and then any irreducible $\mathbb{F}_p H$-module is the restriction to H of an irreducible module for $\Sigma(q)$, by [13, Theorem 13.3]. Here V is irreducible for H, by [3, Lemma 1.3], so we may now assume that $\overline{H}$ is a Chevalley group. If $g = 1$ then $\overline{H}$ may be taken to be $PSL(2, q)$, $q = r^{pm}$, and we then violate Lemma 2.9 via the action of a on a Cartan subgroup of H. On the other hand, suppose that $g \neq 1$, so that $\overline{H} \cong D_4(q)$. As a normalizes a Sylow 3-subgroup of H, there is then an a-invariant maximal subgroup M of H with $M/O_3(M)$ isomorphic to a commuting product of three copies of $SL(2, q)$, permuted transitively by a. There is a section W of V which centralizes $O_3(M)$ and on which $(M/O_3(M))\langle a\rangle$ acts faithfully. By Lemma 2.9, applied to the action of a on $Z(M/O_3(M))$, $M/O_3(M)$ is a central product (with center of order 2). Then a acts on a central product of three quaternion groups in $M/O_3(M)$, permuting the factors, and then once again there is an abelian 2-group on which a acts non-trivially. Thus Lemma 2.9 is violated in any case, and we conclude that $r \neq p$.

We now have $r = 2$ and $p = 3$. Suppose next that $\alpha = f$. There is then an a-invariant subgroup L of H, of Lie rank 1, such that a induces a field automorphism on L. By induction, it follows that $\overline{H}$ itself has Lie rank 1. If $H \cong U_3(2^{3m})$ then again there is an a-invariant subgroup of H isomorphic to $L_2(2^{3m})$, and on which a induces a field automorphism, contrary to induction. If $H \cong L_2(2^{3m})$ or $Sz(2^{3m})$ then a acts non-trivially on the center of a Sylow 2-subgroup of H, contrary to Lemma 2.9. Thus $Z(H) \neq 1$, and

indeed the preceding argument via Lemma 2.9 shows that $Z(H)$ contains a non-identity 2-group. Then $\overline{H} \cong Sz(8)$, by Proposition 3.12, and then Lemma 3.14 implies that a acts non-trivially on $Z(H)$. Again, this outcome is contrary to Lemma 2.9.

We conclude that $\alpha \neq f$. Then Proposition 3.6 yields either $\overline{H} \cong D_4(q)$ and $g \neq 1$, or $\overline{H} \cong {}^3D_4(q)$. If $Z(H) \neq 1$ then Proposition 3.12 and Lemma 3.14 yield $\overline{H} \cong D_4(2)$, $Z(H) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and a acts non-trivially on $Z(H)$, contrary to Lemma 2.9. Thus $Z(H) = 1$. As a lies in an $SL(2,3)$-subgroup of G, there exists a maximal 2-local subgroup M of $H\langle a\rangle$ containing a. Set $L = O^{2'}(M)$. Then $M \cap H$ is a parabolic subgroup of H, and $[Z(O_2(M)), a] = 1$. In particular, we have $[Z(S), a] = 1$ for some Sylow 2-subgroup S of L, and S is also a Sylow 2-subgroup of G. We may then choose M so that $M \cap H$ is the maximal parabolic subgroup $N_H(Z(S))$, and then $L/O_2(L)$ is isomorphic to a direct product of three copies of $PSL(2,q)$ permuted transitively by a (in the $D_4(q)$ case), or to $L_3(q^3)$ (in the ${}^3D_4(q)$ case). A Sylow 3-subgroup of $L\langle a\rangle$ is then contained in a complement to $O_2(L)$, so in either case we find that a acts non-trivially on an abelian 2-subgroup of L. Again Lemma 2.9 yields a contradiction, and the lemma is thereby proved. □

Lemma 4.3. *Assume Hypothesis* 1.1, *and suppose that* $\overline{G}$ *is an alternating group of degree* n. *Then* $|Z(G)| = 2$, *and if* n *is not equal to* 6 *then* $|A| = 3$, *and the non-identity elements of* A *project to* 3*-cycles in* $\overline{G}$.

Proof. Suppose first that $p > 3$. There is then a quasisimple subgroup K of G with $K/Z(K) \cong Alt(p)$ and with $K = [K, a]$. Then two conjugates of a suffice to generate $K\langle a\rangle$, and then Lemma 2.7(a) implies that $p = 5$ and $K \cong SL(2,5)$. If K is contained in an a-invariant subgroup L of G with $L/Z(L) \cong Alt(6)$ then two conjugates of a will generate $L\langle a\rangle$, which is contrary to Lemma 2.7(a). Thus we may assume that n is divisible by 5. If $n = 5$ then there is nothing more to prove, so we may reduce to the case where $\overline{G} \cong Alt(10)$ and where $\bar{a}$ is a product of two disjoint 5-cycles. Here a lies in a subgroup L of G of the form $SL(2,5) \circ SL(2,5)$ (central product with amalgamated centers) and two conjugates of a will then generate a subgroup of L isomorphic to $Alt(5)$. This is again contrary to Lemma 2.7(a). Thus, we need now only consider the case where $p = 3$.

By Hypothesis 1.1, 3 does not divide $|Z(G)|$, and so a classical result of Schur implies that $|Z(G)| \leqslant 2$. Let $a \in A$, $a \neq 1$. Let k be the number of 3-cycles in the standard notation for $\bar{a}$, and suppose first that $k > 1$. As a lies in no Frobenius subgroup of G of order 21, by Lemma 2.9, we then have $n = 3k$. Suppose $k \geqslant 3$, and let $\overline{L}$ be the stabilizer in $\overline{G}$ of $n - 9$ points which are permuted by $\bar{a}$ in three 3-cycles. Then $\overline{L}$ has a subgroup $\overline{K}$ isomorphic to $SL(2,8)$, acting on the nine points of the projective line. Any element of $\overline{L}$ of order 3 is fixed-point-free on these points, so we can choose $\overline{L}$ to be $\bar{a}$-invariant. Denote by L the pre-image of $\overline{L}$ in G, and set $L_0 = [L, L]$. Then $L_0 \cong SL(2,8)$ and $L_0 = [L_0, a]$. But $SL(2,8)$ has no subgroup isomorphic to $SL(2,3)$, so we violate Lemma 2.7(a). Assuming now that $n \neq 6$, we conclude that every non-identity element of A projects to a 3-cycle in $\overline{G}$. Then $|A| = 3$, and since A lies in no subgroup of G which is isomorphic to $Alt(4)$, we obtain $|Z(G)| = 2$. On the other hand, if $n = 6$ and $Z(G) = 1$ then every element of order 3 in G lies in an $Alt(4)$-subgroup of G. Thus we conclude that, in any case, we have $|Z(G)| = 2$. □

Notice that Proposition 4.1 follows from Lemmas 4.2 and 4.3, given our background hypothesis that $\overline{H}$ is a "known" simple group.

5. The case $p > 3$

Our aim in this section is to give a short proof of the following result (which is proved also in [12]).

Theorem 5.1. *Assume Hypothesis* 1.1 *with* $p > 3$. *Then* $G/Z(G)$ *is a group of Lie type in characteristic* p.

We fix notation as in Section 1, so that $H = F^*(G)$ is a quasisimple group, and we have $\overline{G} = G/Z(H)$. Assume Hypothesis 1.1, and fix a non-identity element a of A. Take G to be a minimal counter-example to Theorem 5.1. The following result is then immediate.

Lemma 5.2. *Let* K *be a proper quasisimple subgroup of* H, *with* $K = [K, a]$. *Then* $K/Z(K)$ *is a group of Lie type in characteristic* p.

Lemma 5.3. $\overline{H}$ *is not a sporadic group.*

Proof. Suppose false. Then the outer automorphism group of $\overline{H}$ is of order at most 2, and so $G = H$. Suppose first that $|C_{\overline{G}}(\bar{a})|$ is even. Let $\bar{t}$ be an involution in $C_{\overline{G}}(\bar{a})$, and set $\overline{C} = C_{\overline{G}}(\bar{t})$. As $p > 3$, Lemma 2.9 implies that $F^*(\overline{C}) \neq O_2(\overline{C})$, and it follows from [6, Table 5.3] that $\overline{C}$ has a component $\overline{K}$ with $\bar{a} \in \overline{K}$. By Lemma 5.2, $\overline{K}/Z(\overline{K})$ is of Lie type in characteristic p, and then [6, Table 5.3] yields $p = 5$, $\overline{K} \cong Alt(5)$, and $\overline{G} \cong M_{12}$, J_1, or J_2. The inverse image K of $\overline{K}$ in G is then isomorphic to $SL(2, 5)$, by Lemma 2.7, so $Z(G) \neq 1$, and so $G \cong 2^{\cdot}M_{12}$ or $2^{\cdot}J_2$. In fact, in both these cases the cited table in [6] gives the extra information that $K \cong \mathbb{Z}_2 \times Alt(5)$, and so we may obtain a contradiction in this way. Alternatively, one may note that M_{12} has cyclic Sylow 5-subgroups and contains $Alt(6)$, so that we contradict Lemma 2.7 in this case. In the case that $\overline{G} \cong J_2$, we have $\langle \bar{a} \rangle$ contained in a subgroup isomorphic to $Alt(4) \times Alt(5)$ (the unique maximal subgroup of $\overline{G}$ containing $\overline{C}$), and thus $|C_{\overline{G}}(\bar{a})|$ is divisible by 3. Of the two classes of subgroups of order 5 in $\overline{G}$, $\langle \bar{a} \rangle$ is then identified as lying in a subgroup isomorphic to $3^{\cdot}Alt(6)$, contrary to Lemma 2.7.

We conclude that $C_{\overline{G}}(\bar{a})$ is of odd order. Now Lemma 2.8 implies that G has non-cyclic Sylow p-subgroups. Another trip through the cited table in [6] shows, however, that for any element g of prime order p in a sporadic group X, if X has non-cyclic Sylow p-subgroups then $C_X(g)$ is of even order. This yields the desired contradiction. □

Lemma 5.4. G *is not isomorphic to* $SL(2, r^n)$ *for any* n.

Proof. Immediate from Lemma 2.8. □

Lemma 5.5. $\overline{H}$ *is not a group of Lie type in characteristic* r *different from* p.

Proof. Suppose false. By Proposition 4.1, A induces a subgroup of $Inndiag(\overline{H})$. Let $1 \neq a \in A$, and suppose first that $|C_{\overline{H}}(\bar{a})|$ is of even order. Let $\bar{t}$ be an involution in $C_{\overline{H}}(\bar{a})$. If $r = 2$ then Lemma 3.11 implies that $C_{\overline{G}}(\bar{t})$ is 2-constrained, and we contradict Lemma 2.9. Thus $r \neq 2$. If $\overline{H} \cong PSL(2, r^n)$ then $H \cong SL(2, r^n)$ since H involves $SL(2, p)$, and we then contradict Lemma 5.4. Thus $\overline{H}$ is not isomorphic to $PSL(2, r^n)$, and then by Lemmas 3.8 and 3.7 there is a subnormal subgroup $\overline{K}$ of $C_{\overline{H}}(\bar{t})$, with $\overline{K}$ of Lie type in characteristic r. As $p > 3$ and $r \neq 2$ there are no isomorphisms between any members of $Lie(r)$ and $Lie(p)$, and so $\overline{K} \notin Lie(p)$. If $[\overline{K}, \bar{a}] = 1$ then $\bar{a}$ is in an r-local subgroup of $\overline{G}$, and we again contradict Lemma 2.9 via the Borel–Tits theorem. Thus, $[\overline{K}, \bar{a}] \neq 1$. Then Lemma 5.2 implies that $\langle (\overline{K})^{\langle \bar{a} \rangle} \rangle$ is a product of p components of $C_{\overline{H}}(\bar{t})$, or a commuting product of p copies of $SL(2, 3)$ or of $L_2(3)$. Again, the result is that $\bar{a}$ lies in an r-local subgroup of $\overline{G}$, and a contradiction ensues. We therefore conclude that $C_{\overline{G}}(\bar{a})$ is of odd order.

Now Lemma 2.8 shows that G has non-cyclic Sylow p-subgroups. As p is odd, there is then an elementary abelian subgroup $\overline{B}$ of $\overline{G}$ of order p^2, with $\bar{a} \in \overline{B}$. Then Lemma 3.9 implies that $O^{r'}(C_{\overline{H}}(\bar{b})) \neq 1$ for some $\bar{b} \in \overline{B}$. By Lemma 3.7 we then have $O^{r'}(C_{\overline{H}}(\bar{b})) = \overline{L}_1 \cdots \overline{L}_m$, where each $\overline{L}_i$ is a group of Lie type in characteristic r, and where $[\overline{L}_i, \overline{L}_j] = 1$ for all $i \neq j$. Here $O^{r'}(C_{\overline{H}}(\bar{b}))$ is $\bar{a}$-invariant, and since we have already seen that $\bar{a}$ lies in no r-local subgroup of $\overline{G}$, we conclude that each $\overline{L}_i$ is $\bar{a}$-invariant and that $[\overline{L}_i, \bar{a}] \neq 1$. Now Lemma 5.2 implies that each $\overline{L}_i$ is solvable, and since $p > 3$ it then follows that $\overline{L}_i$ has no automorphisms of order p. Then $[\overline{L}, \bar{a}] = 1$, and we have a contradiction. □

Notice that Lemma 4.3, and Lemmas 5.2 through 5.5, yield Theorem 5.1.

6. Cross-characteristic Lie type groups, $p = 3$

In this section we assume Hypothesis 1.1 with $p = 3$. As always, we set $\overline{G} = G/Z(G)$ and $H = E(G)$. We shall assume further that $\overline{H}$ is a group of Lie type in characteristic different from 3. Indeed, we even wish to assume that there exists no exceptional isomorphism of $\overline{H}$ with a group of Lie type in characteristic 3. Thus, $\overline{H}$ is not isomorphic to $Sp(4, 2)'$ ($\cong L_2(9)$), $G_2(2)'$ ($\cong U_3(3)$), or $U_4(2)$ ($\cong PSp(4, 3)$).

By a "parabolic subgroup" of H, we mean the complete inverse image in H of a bona fide parabolic subgroup of $H/Z(H)$. Similarly, we have the notions of "Borel subgroup," "Cartan subgroup," and of " root group" in H.

Our goal, in this section, is the following result.

Theorem 6.1. *Assume Hypothesis* 1.1, *with $H/Z(H)$ a group of Lie type, and not isomorphic to a group of Lie type in characteristic* 3. *Then either G is isomorphic to one of the groups $PGU(n, 2)$, $n \geqslant 5$, or else $|Z(G)| = 2$, and $\overline{G}$ is isomorphic to one of the groups $L_2(4)$, $L_4(2)$, $Sp(6, 2)$, $D_4(2)$, or $G_2(4)$. Moreover, we have $|A| = 3$ in every case.*

For the remainder of this section, let G be a minimal counter-example to Theorem 6.1. Throughout, let r denote the defining characteristic of $\overline{H}$, $r \neq 3$, and fix a non-identity element $a \in A$.

Lemma 6.2. *Suppose that the Lie rank of $H/Z(H)$ is equal to* 1. *Then $G \cong 2^{\cdot}L_2(4)$.*

Proof. By Lemma 4.2, A induces inner-diagonal automorphisms on $\overline{H}$. Thus $|Inndiag(\overline{H})|$ is divisible by 3, and so $\overline{H}$ is not isomorphic to $Sz(2^n)$. Also, as $r \neq 3$, by assumption, $\overline{H}$ is not a Ree group in characteristic 3. Thus $\overline{H} \cong PSL(2,q)$ or $PSU(3,q)$ for some q, $q = r^n$.

Suppose first that $\overline{H} \cong PSL(2,q)$. Then $|Inndiag(H) : \overline{H}| \leqslant 2$, so $A \leqslant H$, and so $H = G$. As G involves $SL(2,3)$, we conclude that $|Z(G)| = 2$. Assuming that $\overline{G}$ is not isomorphic to $SL(2,4)$, it follows from Proposition 3.12 that r is odd. Thus $r \geqslant 5$, and since $2^{\cdot}SL(2,4) \cong SL(2,5)$ we have $q > 5$. Put $d = q-1$, and let λ be a primitive dth root of unity in $\mathbb{F}_q$. Then take:

$$a = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & \lambda^{-1} \\ -\lambda & -1 \end{pmatrix}$$

and obtain

$$ab = \begin{pmatrix} \lambda & 1-\lambda^{-1} \\ 0 & \lambda^{-1} \end{pmatrix}.$$

Here b is of order 3, so b is conjugate to a in G. By Lemma 2.6, we have $\langle a, b\rangle$ isomorphic to $SL(2,3)$ or $SL(2,5)$, and so $|ab| \leqslant 5$. But ab has order $q-1$, so we conclude that $q \leqslant 6$, and then $q = 5$, contrary to our choice of q.

Suppose next that $\overline{H} \cong PSU(3,q)$. Let L_0 be a subgroup of H with $L_0 = \langle a^{L_0}\rangle \cong SL(2,3)$. Let t be the involution in L_0, and set $L = O^{r'}(C_H(t))$. Then $L \cong SL(2,q)$, and $[L,a] \neq 1$. By what has already been shown in the preceding paragraph, we then have $q = 5$. Both $SU(3,5)$ and $PGU(3,5)$ have extraspecial Sylow 3-subgroups of exponent 3. In particular, all subgroups of order 3 in $PGU(3,5)$ which are contained in $PSU(3,5)$ are conjugate. By the Frattini argument, the normalizer in $PGU(3,5)$ of a Sylow 5-subgroup contains such an "outer" subgroup of order 3, so we must conclude from Lemma 2.9 that $a \in H$. One may deduce from the action of $SU(3,5)$ on its natural module that all subgroups of order 3 in $PSU(3,5)$ are conjugate. As $PSU(3,5)$ contains a Frobenius group of order 21, we again contradict Lemma 2.9. □

Lemma 6.3. *$\overline{H}$ is not isomorphic to $PSL_3(q)$ for any power q of r.*

Proof. Suppose $\overline{H} \cong PSL_3(q)$, $q = r^n$. As always, we have a subgroup X of G containing a, with $X \cong SL(2,3)$. Consider first the case where $Z(H) = 1$. If r is even, then the centralizer in G of any non-identity 2-subgroup of G is contained in a parabolic subgroup of G, while if r is odd then G has a unique conjugacy class of involutions. In either case we find that $C_G(Z(X))$ is contained in a proper parabolic subgroup P of G. Here $O_r(P)$ is abelian, and then Lemma 2.9 yields $a \in C_G(O_r(P))$, whereas $O_r(P) \geqslant C_G(O_r(P))$.

We conclude that $Z(H) \neq 1$. As G acts irreducibly on V, $|Z(H)|$ is prime to 3, so Proposition 3.12 implies that $\overline{H} \cong L_3(4)$ and $Z(H)$ is a 2-group. Since a centralizes $Z(H)$, we conclude from Lemma 3.14 that $a \in H$. As all elements of order 3 in $L_3(4)$ are conjugate, and as $L_3(4)$ contains a Frobenius group of order 21, we contradict Lemma 2.9. This proves the lemma. □

Lemma 6.4. *If the Lie rank of $\overline{H}$ is at least 2 then $r = 2$, and a normalizes a maximal parabolic subgroup of $\overline{H}$.*

Proof. Assume that the Lie rank of $\overline{H}$ is at least 2. Then $\bar{a}$ lies in an r-local subgroup $\overline{N}$ of $\overline{G}$, by Lemmas 6.3 and 3.8. By Lemma 3.11(a), $\overline{N}$ is r-constrained, so Lemma 2.9 implies that $r = 2$. By Lemma 3.11(b) we may choose $\overline{N}$ so that $\overline{N} \cap \overline{H}$ is a parabolic subgroup of $\overline{H}$. Let $\overline{P}$ be an a-invariant, proper parabolic subgroup of $\overline{H}$. As a induces an inner-diagonal automorphism of $\overline{H}$ we may write $a = xd$ where $x \in P$ and where $d \in N_G(\overline{S})$ where $\overline{S}$ is a Sylow r-subgroup of $\overline{P}$. Then any maximal parabolic subgroup of $\overline{H}$ containing $\overline{P}$ is a-invariant. □

For the remainder of this section we assume that the Lie rank of G is at least 2. Thus $r = 2$, by Lemma 6.4. Fix a Borel subgroup B of H, and let Σ (resp. Σ^+) be the root system (resp. the positive subsystem) associated with H and with B, so that $O_2(B)$ is generated by the root groups X_α, $\alpha \in \Sigma^+$. If P is a parabolic subgroup of H containing B then the set of simple roots $\alpha \in \Sigma^+$ such that $X_{-\alpha} \leqslant P$ will be denoted $\mathcal{D}(P)$. We take $\mathcal{D}(P)$ to have also the structure of a graph, with incidence induced from the Coxeter diagram of Σ, and we say that P is *connected* if $\mathcal{D}(P)$ is connected. More generally, let $\mathcal{D}_1, \ldots, \mathcal{D}_r$ be the connected components of $\mathcal{D}(P)$, and for each i, $1 \leqslant i \leqslant r$, put

$$L_i = \langle X_\alpha, X_{-\alpha} \colon \alpha \in \mathcal{D}_i \rangle \quad \text{and} \quad \Lambda = \Lambda(P) = \{L_1, \ldots, L_r\}.$$

We will refer to the members of $\Lambda(P)$ as the *Levi complements* of P, relative to Σ.

Lemma 6.5. *Assume that the Lie rank of G is at least 2. Then there is a Sylow 2-subgroup S of H, and a proper parabolic subgroup P of G containing $\langle N_H(S), a\rangle$, for which the following condition holds.*

$$\text{For every } L \in \Lambda(P) \text{ we have } 1 \neq [a, L] \leqslant L. \tag{$*$}$$

Moreover, we can choose P so that the Lie rank of each L in $\Lambda(P)$ is equal to 1.

Proof. By Lemma 6.4, a normalizes a maximal parabolic subgroup N of H. If $[N, a] \leqslant O_2(N)$ then a normalizes a Sylow 2-subgroup of N (hence of H), and then a normalizes every parabolic subgroup of H containing S. In particular, there is then a rank-1 parabolic subgroup P of H, invariant under a, and with $[O^{2'}(P), a] \not\leqslant O_2(P)$. Thus, the desired conclusion holds in this case, and we may therefore assume that $[N, a] \not\leqslant O_2(N)$.

Among all a-invariant parabolic subgroups N with $[N, a] \not\leqslant O_2(N)$, choose N so that the Lie rank of N is as small as possible. We then construct the set $\Lambda(N) = \{L_1, \ldots, L_t\}$ of Levi complements in N, relative to a fixed Borel subgroup of N. Then $N = O_2(N)L_1 \cdots L_t K$, for some Cartan subgroup K of B, and we may assume (possibly after replacing a by a conjugate) that a normalizes $L_1 \cdots L_t K$. As a is inner-diagonal, a normalizes each L_i, and if $[a, L_i] = 1$ for some i we contradict the minimality of N. This proves the first part of the lemma. But further, if the Lie rank of some L_i is bigger than 1, then we may apply induction on the Lie rank, with $L_i\langle a\rangle$ in place of G, to conclude

that $L_i\langle a\rangle$ has a proper parabolic subgroup containing a. From this we again contradict the minimality of N, and thus each L_i has Lie rank equal to 1. □

Lemma 6.6. *Assume that the Lie rank of $\overline{H}$ is at least 2, and assume that the field of definition for $\overline{H}$ (in the sense of a σ-setup, as in Section 3) is larger than $\mathbb{F}_2$. Then $G \cong 2^{\cdot}G_2(4)$, and $|A| = 3$. Moreover, we have $A = Z(R)$ for some Sylow 3-subgroup R of G, and $C_G(A) \cong SL(3,4)$.*

Proof. By Lemma 6.5 there exists a proper parabolic subgroup P of G, and a Levi complement L in P, such that $L \geqslant [L,a] \neq 1$. Since the field of definition of $\overline{G}$ is larger than $\mathbb{F}_2$, we may apply Lemma 6.2 to $L\langle a\rangle$ and obtain $L \cong 2^{\cdot}L_2(4)$. Here $L \notin Lie(2)$, so $Z(L) \leqslant Z(H)$. Then Proposition 3.12 and Lemma 6.3 yield $G \cong 2^{\cdot}G_2(4)$.

Let R be a Sylow 3-subgroup of G containing A. Then $|R| = 27$, and R is contained in an $SL(3,4)$ subgroup X of $G_2(4)$. Every element of $R - Z(R)$ is contained in a Frobenius subgroup of X of order 21, so Lemma 2.9 implies that $A = Z(R)$ is of order 3. We observe that A is contained in a Cartan subgroup D of X, which is a Cartan subgroup of G. The Chevalley relations imply that X is generated by the set of root subgroups centralized by A, relative to the root system determined by D. Then $X = O^{2'}(C_G(A))$, and $C_G(A) = XD = X$. □

For the remainder of this section we assume that the Lie rank of $\overline{H}$ is at least 2, and that $\mathbb{F}_2$ is the field of definition for $\overline{H}$. Further, we assume that there exists no exceptional isomorphism between $\overline{H}$ and a group in $Lie(3)$. By Lemma 6.5, we may fix a parabolic subgroup P of G containing a, such that condition $(*)$ in Lemma 6.5 holds, and such that every member of $\Lambda(P)$ is of Lie rank 1. Let $\mathcal{M}$ be the set of all maximal parabolic subgroups of H containing P, and having the property that every connected component of the diagram $\mathcal{D}(M)$ contains at least one vertex of $\mathcal{D}(P)$. One readily verifies that $\mathcal{M}$ is non-empty, and we fix $M \in \mathcal{M}$.

Lemma 6.7. *The following hold.*

(a) *We have $[L,a] \neq 1$ for any $L \in \Lambda(M)$.*
(b) *We have $\langle a^M\rangle \geqslant O^{2'}(M)$.*
(c) *Let S be a Sylow 2-subgroup of M, and suppose that $Z(S) \not\leqslant Z(H)$. Then $M = N_H(Z(S))$, and $\mathcal{M} = \{M\}$.*

Proof. Part (a) is immediate from the definition of $\mathcal{M}$. Then $L \leqslant \langle a^L\rangle$ for any $L \in \Lambda(M)$, and (b) follows. Suppose that $Z(S) \not\leqslant Z(H)$. We have $[Z(O_2(M)), a] = 1$ by Lemma 2.9, and it follows from part (b) that $[Z(O_2(M)), O^{2'}(M)] = 1$. Then $Z(S) \trianglelefteq M$, and then since M is a maximal parabolic we have $M = N_H(Z(S))$. This yields (c). □

Lemma 6.8. *Suppose that $\overline{H}$ is isomorphic to $PSU(n,2)$ $n \geqslant 5$. Let ϕ be the canonical homomorphism from $GU(n,2)$ onto $PGU(n,2)$, and let U be the natural module for $GU(n,2)$ over $\mathbb{F}_4$. Then $G \cong PGU(n,2)$, $|A| = 3$, and $a = \phi(a^*)$ for some element $a^* \in GU(n,2)$ such that $C_U(a^*)$ has codimension 1 in U.*

Proof. Let S be a Sylow 2-subgroup of M. It follows from Lemma 3.14 that $Z(S) \not\leqslant Z(G)$, so Lemma 6.7(b) yields $M = N_H(Z(S))$. Then $O_2(\overline{M})$ is extraspecial of width $n-2$, and $O^{2'}(\overline{M}/O_2(\overline{M}))$ is isomorphic to $SU(n-2,2)$. Further, as $O_3(G) = 1$ and $Z(G)$ is cyclic, it follows from Proposition 3.12 that $|Z(G)| \leqslant 2$, and that $Z(G) = 1$ if $n \neq 6$. Then Lemma 3.13 implies that $O_2(M) = X \times Z(G)$, where X is a central product of $n-2$ quaternion groups.

Set $Y = [O_2(M), a]$. We have $\Phi(Y) \leqslant Z(X)$, so Y is contained in an extraspecial subgroup of $O_2(M)$, and then Lemma 2.9 implies that Y is a quaternion group. From this we may conclude that $M/O_2(M)Z(G)$ is isomorphic to $GU(n-2,2)$, and then $\overline{G} \cong PGU(n,2)$. In particular, if 3 divides n then $a \notin H$, and so Lemma 3.14 yields $Z(G) = 1$. Thus $O_2(M) = X$, and $C_X(a)$ is a central product of $n-3$ quaternion groups. It follows that $O^{2'}(C_G(a)) \cong SU(n-1,2)$. Set $G^* = GU(n,2)$, let U be the natural module for G^* over $\mathbb{F}_4$, and let a^* be a pre-image of a in G^*. Then $O^{2'}(C_{G^*}(a^*)) \cong SU(n-1,2)$, and we may choose a^* so that $C_U(a^*)$ has codimension 1 in U.

Suppose that $|A| > 3$. Then $C_G(a) = \langle A^{C_G(a)} \rangle$, and so

$$0 = \big[V, a, C_G(a)\big] = \big[V, C_G(a), C_G(a)\big].$$

Then $[C_G(a), C_G(a)]$ centralizes V, by the Three Subgroups Lemma. But $C_G(a)$ is non-abelian, as $n > 3$. Thus $|A| = 3$, and all parts of the lemma have been established. □

Lemma 6.9. *Assume that $\overline{H}$ is defined over $\mathbb{F}_2$, that $\overline{H}$ is not a unitary group $PSU(n,2)$ with $n \geqslant 5$, and that $\overline{H}$ cannot be viewed (via an exceptional isomorphism) as a group of Lie type in characteristic* 3. *Then $|Z(G)| = 2$, and $\overline{G}$ is isomorphic to $\Omega_4^-(2)$, $L_4(2)$, $Sp(6,2)$, or $D_4(2)$.*

Proof. As A induces inner-diagonal automorphisms on $\overline{H}$, it follows that $H = G$ or that $\overline{H} \cong {}^2E_6(2)$. Suppose first that $\overline{G}$ is isomorphic to $L_n(2)$ or $Sp(2n,2)$. If $Z(G) \neq 1$ then Proposition 3.12 and Lemma 6.3 yield $G \cong 2 \cdot L_4(2)$ or $2 \cdot Sp(6,2)$, and thus the lemma holds in this case. On the other hand, if $Z(G) = 1$ then $C_G(Z(S))$ is not a maximal parabolic subgroup of G, and we contradict Lemma 6.7(b). Thus, we may assume that $\overline{G}$ is not isomorphic to $L_n(2)$ or $Sp(2n,2)$.

Suppose that $\overline{G}$ is an orthogonal group $\Omega_{2n}^{\varepsilon}(2)$, and let U be a natural module for $\overline{G}$ over $\mathbb{F}_2$, of dimension $2n$. As G is non-solvable we have $n \geqslant 2$, and $n \geqslant 3$ if $\varepsilon = +1$. In view of Lemma 6.2, and the isomorphism of $\Omega_4^-(2)$ with $SL(2,4)$, we need only consider the cases where $n \geqslant 3$. As $\Omega_6^+(2) \cong L_4(2)$, and $\Omega_6^-(2) \cong PSp(4,3)$, we may in fact take $n \geqslant 4$. If $Z(H) \neq 1$, then Proposition 3.12 yields $\overline{G} \cong D_4(2)$ (which is isomorphic to $\Omega_8^+(2)$), and then since $Z(G)$ is cyclic, Proposition 3.12 yields $|Z(G)| = 2$. Thus, the lemma holds in this case, and so we may assume that $Z(G) = 1$.

Let U_0 be a totally singular subspace of U, of dimension 2, and denote by L the stabilizer in G of U_0. Without loss, we may assume that a Sylow 2-subgroup S of L is contained in M. With the aid of Witt's Theorem on extensions of isometries, we find that $L = X(K_1 \times K_2)$, where $X = O_2(L)$, $K_1 \cong \Omega_{2n-4}^{\varepsilon}(2)$ and $K_2 \cong L_2(2)$. Further, X is extraspecial, of width $2n-4$, and $X/Z(X)$ is isomorphic, as a module for K_1K_2, to a tensor product $N_1 \otimes N_2$, where N_i is a natural module for K_i over $\mathbb{F}_2$. In particular, L is a maximal

parabolic subgroup of G, and $Z(S) = Z(L)$, so $L = M$ by Lemma 6.7(b), and $a \in L$. Now let N_0 be an irreducible K_1-submodule of $X/Z(X)$. Then $X/Z(X) = N_0 \oplus (N_0)^g$ for any $g \in K_1K_2 - K_1$. For any element d of K_1 of order 3 we then have $|[X/Z(X), d]| \geqslant 16$, and so $[X, d]$ is not a quaternion group. Thus $a \notin K_1$, by Lemma 2.9. But, for any element d of $K_1K_2 - K_1$ of order 3, we have $|[X/Z(X), d]| \geqslant |N_0|$, where $|N_0| \geqslant 16$ as $n \geqslant 4$. As a is conjugate to an element of K_1K_2, we have a contradiction at this point. Thus, we may assume that $\overline{H}$ is not an orthogonal group.

As $\overline{H}$ is not a unitary group (the case of $U_4(2) \cong \Omega_6^-(2)$ having been treated above), we now conclude that $\overline{G}$ is not a classical group. If $\overline{G} \cong E_n(2)$ ($n = 6, 7, 8$), then $|Z(G)|$ is odd, and so $|\mathcal{M}| = 1$, by Lemma 6.7. Recall, however, that $\mathcal{M}$ is the set of maximal parabolic subgroups M of H containing P, where P is a totally disconnected parabolic subgroup of H, and where each connected component of M contains at least one vertex of $\mathcal{D}(P)$. One has only to glance at the diagrams for the groups $E_n(2)$, however, to see that in fact $|\mathcal{M}| > 1$ for any choice of P. Thus, $\overline{G} \ncong E_n(2)$. Suppose that $\overline{G} \cong {}^2F_4(2)'$. Then again $Z(G) = 1$ and $\mathcal{M} = \{C_G(Z(S))\}$. Then $M/O_2(M) \cong Sz(2)$, and so $|M|$ is prime to 3, contrary to $a \in M$. By a similar argument, if $\overline{H} \cong {}^3D_4(2)$ then $|Z(G)| = 1$ and $a \in M = C_G(Z(S))$, so that M has an a-invariant Levi complement isomorphic to $SL(2, 8)$. But this result is excluded by Lemma 6.2. As $G_2(2)'$ may be viewed as a group in characteristic 3, we come finally to $\overline{G} \cong F_4(2)$ or $\overline{H} \cong {}^2E_6(2)$. Then $\mathcal{D}(G)$ is the F_4 diagram, and since $\mathcal{D}(P)$ is totally disconnected we can choose $M \in \mathcal{M}$ so that $\mathcal{D}(M)$ contains a subdiagram of type A_2. There then exists $L \in \Lambda(M)$ with $L/Z(L) \cong L_3(2)$ or $L_3(4)$. Replacing G by $L\langle a\rangle$, we obtain a contradiction from Lemma 6.3. □

Lemma 6.10. *If $\overline{G} \cong L_4(2)$, $Sp(6, 2)$, $G_2(4)$, or $D_4(2)$ then $|A| = 3$.*

Proof. Suppose, by way of contradiction, that $|A| = 9$. If $\overline{G} \cong L_4(2)$ it follows that both classes of elements of order 3 in G are represented in A, and since G contains a Frobenius group of order 21, we contradict Lemma 2.9.

Suppose next that $\overline{G} \cong Sp(6, 2)$, and let U be the natural module for $\overline{G}$ over $\mathbb{F}_2$. If there exists a in A with $|[U, \bar{a}]| \neq 16$ then $\bar{a}$ is contained in an $L_3(2)$-subgroup of $\overline{G}$, contrary to Lemma 6.3. On the other hand, we have $U = \langle C_U(\bar{a})\colon\ 1 \neq \bar{a} \in \overline{A}\rangle$, so there exist $a, b \in A$ such that $|[U, \bar{a}]| = |[U, \bar{b}]| = 4$, and with $\langle a, b\rangle = A$. Then $|[U, \overline{ab}]| = 16$, and so we have a contradiction in this case.

The case where G is isomorphic to $G_2(4)$ was already considered in Lemma 6.6. So, finally, suppose that $\overline{G} \cong D_4(2)$, and let U be a natural $O_8^+(2)$-module for $\overline{G}$. We claim that there exists $a \in A$ with $16 \leqslant |[U, a]| \leqslant 64$. Suppose false. Then $|[U, a]| = 4$ or 2^8 for every non-identity element $a \in A$. Let a and b generate A. If $|[U, a]| = |[U, b]| = 4$ then $|[U, ab]| = 16$, while if $|[U, a]| = 4$ and $|[U, b]| = 2^8$ then either $[U, ab]$ or $[U, ab^2]$ is of order 64. The only other case is that in which $C_U(a) = 0$ for every non-identity $a \in A$, which is absurd. The claim is therefore established. Now fix $a \in A$ with $|[U, a]| = 16$ or 64. There is then a non-degenerate a-invariant subspace W of V, of type $O_6^+(2)$, with $|[W, a]| = 16$. Let H be the point-wise stabilizer in G of $W^\perp$. Then $H \cong \Omega_6^+(2) \cong Alt(8)$, and we have $H = [H, a]$. Identifying H with $Alt(8)$, and identifying W with the non-trivial irreducible constituent in the natural permutation module for $Alt(8)$, it follows that

a induces on W the action of a product of two disjoint 3-cycles. There is then a 7-cycle x in H with $x^a = x^2$. This contradicts Lemma 2.9, so the lemma is proved. □

Theorem 6.1 follows from Lemmas 6.2 through 6.10.

7. Sporadic groups, $p = 3$

We continue to assume Hypothesis 1.1, with $p = 3$. Further, we assume that $\overline{H}$ is among the 26 sporadic simple groups. The index of $\overline{H}$ in its automorphism group is then at most 2, and then since $G = \langle A^G \rangle$ we have $G = H$. Also, since $O_3(G) = 1$, the only cases in which $Z(G) \neq 1$ occur when $Z(G)$ is of order 2 or (in the unique case of M_{22}) of order 4. We will obtain the following result.

Theorem 7.1. *Assume Hypothesis* 1.1, *with* $\overline{G}$ *a sporadic simple group. Then* $G \cong 2^{\cdot}J_2$, $2^{\cdot}Suz$, *or* $2^{\cdot}Co_1$, *and we have* $|A| = 3$.

We will make free use of the tables in Section 5.3 of [6], in which, for each sporadic group X, and each subgroup Y of X of prime order, the normalizer $N = N_X(Y)$ is determined, in the sense that a chief series for N is given, along with the action of N on the various chief factors. Also, we will draw on the character tables in the ATLAS of Finite Groups [4], in order to establish that $2^{\cdot}Co_1$ contains a perfect central extension $6^{\cdot}Suz$, and that $2^{\cdot}Suz$ contains a perfect central extension $6^{\cdot}U_4(3)$.

Six cases may be eliminated right away. Namely, by Lemma 2.9, if G has a unique conjugacy class of subgroups of order 3, then G does not contain a Frobenius subgroup of order 21. In this way, we obtain the following result.

Lemma 7.2. $\overline{G}$ *is not isomorphic to* M_{22}, M_{23}, J_1, HS, Ru, *or* $O'N$.

We next observe, that the centralizer of any element of order 3 in any sporadic group is of even order. In particular, $|C_{\overline{G}}(a)|$ is even. For the remainder of this section, we fix an element t of $C_G(a)$ with $\bar{t}$ of order 2. Set $\overline{C} = C_{\overline{G}}(\bar{t})$, and denote by C the inverse image of $\overline{C}$ in G. Also, set $K = \langle a^C \rangle$, and set $R = F^*(K)$. We will proceed by induction on $|G|$.

Definition 7.3. Let X be a group, and set $R_0 = F^*(X)$. We say that X is of *extraspecial type* if the following three conditions hold.

(i) $R_0 = Z(R_0)E$ where R_0 is an extraspecial group of width $n \geqslant 2$.
(ii) X/R_0 is isomorphic to one of the groups $Alt(2n+1)$, $Alt(2n+2)$, $GU(n,2)$, $\Omega_{2n}^{\varepsilon}(2)$ (for some sign ε), or $Sp(2n,2)$, and
(iii) $R_0/Z(R_0)$ is a natural (irreducible) $\mathbb{F}_2$-module for K/R_0.

Lemma 7.4. *The following hold.*

(a) *If K is quasisimple then $K/O_3(K)$ is in the list of quasisimple groups which are outcomes in Theorem* 1.2.
(b) *If $R = Z(R)E$ is a 2-group where E is extraspecial of width $n \geqslant 2$, then K is of extraspecial type, in the sense of Definition* 7.3.

Proof. Part (a) is by induction on $|G|$. Part (b) is immediate from [3, Theorem A]. □

Before going to work with Lemma 7.4, it will be convenient to eliminate eight more groups by considering 5-local subgroups.

Lemma 7.5. *$\overline{G}$ is not isomorphic to Mc, Co_3, Co_2, Ly, F_5, F_3, F_2, or F_1.*

Proof. We first show that in each of the above possibilities for $\overline{G}$ we have $|C_G(a)|$ divisible by 5. Indeed, in the cases other than $\overline{G} \cong Mc$, F_3, or Co_3, one checks that the centralizer of every element of order 3 has a subgroup of order 5.

Suppose that $\overline{G} \cong Mc$. Then $Z(G) = 1$, G has one class of involutions, and then $C_G(t) \cong 2{\cdot}A_8$. Then $C_G(\langle a, t\rangle) \cong \mathbb{Z}_3 \times SL(2,5)$, by Lemma 4.3, and thus $|C_G(a)|$ is divisible by 5 in this case.

Suppose next that $\overline{G} \cong F_3$. Then $Z(G) = 1$, G has just one conjugacy class of involutions, and we have $C_G(t)$ of the form $2^{1+8}_+.Alt(9)$. Now [3, Theorem B] shows that a is incident with a 3-cycle in $C_G(t)/O_2(C_G(t))$, and so we again get 5 dividing the order of $C_G(a)$.

Suppose that $\overline{G} \cong Co_3$ and that 5 does not divide the order of $C_G(a)$. Again, we have $Z(G) = 1$, and we find that $C_G(a) \cong \mathbb{Z}_3 \times L_2(8) : 3$. In particular, a is not contained in the commutator subgroup of $C_G(a)$. Now consider $C = C_G(t)$. By Lemma 7.4(a), C is not isomorphic to $\mathbb{Z}_2 \times M_{12}$. This leaves only the case $C \cong 2{\cdot}Sp(6,2)$. Let U denote the natural $Sp(6,2)$-module for C. As 5 does not divide $|C_G(a)|$ we have $|[U,a]| > 4$, and since a is not in the commutator subgroup of $C_G(a)$ we have $|[U,a]| \neq 64$. This leaves $|[U,a]| = 16$. But then a lies in a Frobenius 21-subgroup of G, and we have a contradiction via Lemma 2.9. Thus, we have found that $|C_G(a)|$ is divisible by 5 in all cases under consideration.

Let F be a subgroup of $C_G(a)$ of order 5. Then $C_{\overline{G}}(\overline{F})$ is not 5-constrained, by Lemma 2.9. We consult [6, Table 5.3] for the structure of centralizers of elements of order 5. setting $D = O^{3'}(C_G(F))$, we have $D \neq 1$. Further, D is not isomorphic to $Alt(5)$ (as follows from Lemma 2.4) or to $U_3(5)$ (by Theorem 6.1), or to HS or F_5 (by induction in Theorem 7.1). But in fact, as one checks, this exhausts the list of possibilities for the structure of $C_G(F)$, and so Lemma 7.5 is proved. □

Lemma 7.6. *$\overline{G}$ is isomorphic to J_2, Suz, or Co_1.*

Proof. We shall go through the list of groups, and check the conditions in Lemma 7.3 against the structure of the centralizers of involutions in the sporadic groups that remain to be considered. In view of Lemmas 7.2 and 7.5, these are (aside from the three groups

mentioned in the statement of the lemma) the nine groups Fi'_{24}, Fi_{23}, Fi_{22}, He, J_4, J_3, M_{24}, M_{12}, and M_{11}. We note that, among these nine groups, only Fi_{22}, and M_{12} have non-trivial Schur multipliers, and in these two cases the multiplier is of order 2.

We begin with $G \cong Fi'_{24}$. Here there are two classes of involutions, and we find that either K is double cover of Fi_{22} or R is an extraspecial 2-group of width 6 with K/R isomorphic to $3U_4(3)$. In both these cases, we violate Lemma 7.4.

Suppose next that $G \cong Fi_{23}$. In view of Lemma 7.4(a), K is not a Schur extension of Fi_{22} or $U_6(2)$. This leaves only the possibility that C is of the form

$$\big(2^2 \times 2_+^{1+8}\big)\big(\big(GU_4(2)\big)2\big). \tag{1}$$

Then $Z(C/O_2(C))$ is of order 3, acting non-trivially on $Z(O_2(C))$, as follows from the structure of the corresponding involution-centralizer in Fi'_{24}. Thus $K/R \cong U_4(2)$. Here $Z(C/O_2(C))$ acts non-trivially on $R/Z(R)$, so that $R/Z(R)$ is the natural unitary module for K/R. This violates Lemma 7.4(b).

Suppose that $\overline{G} \cong Fi_{22}$. By Lemma 7.4(a), K is not a Schur extension of $U_6(2)$ and examination of the remaining classes of involution centralizers then yields $F^*(C) = O_2(C)$. Further, for any involution $\bar{s}$ of $\overline{G}$ such that $C_{\overline{G}}(\bar{s})$ is 2-constrained, either $C_{\overline{G}}(\bar{s})$ is of the form

$$\big(2 \times 2_+^{1+8}\big)U_4(2) \tag{2}$$

or $C_{\overline{G}}(\bar{s})$ does not contain a Sylow 2-subgroup of G. It follows from Lemma 2.9 that $[Z(S), a] = 1$ for some Sylow 2-subgroup S of G. Since the group in (2) lifts to a subgroup of the group in (1) in Fi_{23}, one observes that there exists a 2-central involution s of G with $s \notin Z(G)$. We may then take $s = t$, whence $\overline{C}$ is as in (2). This violates Lemma 7.4.

In the group He there are two classes of involutions, and we find that either K is a Schur extension of $L_3(4)$ or K is of the form $D_8^{*3} : L_3(2)$. Both these possibilities are excluded by Lemma 7.4 (or by noticing that in both these groups, each element of order 3 lies in a Frobenius group of order 21).

In J_4 there are two classes of involutions, and we find that K is of the form $Q_8^{*6}(3M_{22})$ or $2^{11}M_{22}$, in each case violating of Lemma 7.4.

If G is isomorphic to J_1 or J_3, we obtain $C/O_2(C) \cong Alt(5)$, and C contains a subgroup isomorphic to $Alt(5)$. This violates Lemma 2.7.

In M_{24} there are two classes of involutions, with centralizers of the form $(D_8^{*3})L_3(2)$ and $(2^6)Sym(5)$. Thus, we violate Lemma 7.4 if $G \cong M_{24}$.

If G is isomorphic to M_{11} then G has a single conjugacy class of elements of order 3, and since $M_{11} \geqslant M_{10} \geqslant Alt(6) \geqslant Alt(4)$, we contradict Lemma 2.9.

Finally, suppose that $\overline{G}$ is isomorphic to M_{12}, and let S be a Sylow 3-subgroup of G containing a. Then S is extraspecial of order 27. If $a \in Z(S)$ then every elementary abelian subgroup of order 9 in G contains a conjugate of a, and hence a lies in an M_{11}-subgroup of G, contrary to the preceding paragraph. Thus $a \notin Z(S)$, and one then has $C_{\overline{G}}(\bar{a}) \cong \mathbb{Z}_3 \times A_4$. Let $\bar{s}$ be an involution in $C_{\overline{G}}(\bar{a})$. If $\bar{s}$ is 2-central then $O^2(C_{\overline{G}}(\bar{s})) \cong 2_+^{1+4} : \mathbb{Z}_3$, whereas $C_{\overline{G}}(\langle \bar{a}, \bar{s}\rangle) \cong \mathbb{Z}_6 \times \mathbb{Z}_2$. Thus $\bar{s}$ is not 2-central, and so $C_{\overline{G}}(\bar{s}) \cong \mathbb{Z}_2 \times Sym(5)$.

Then also $\bar{a}$ normalizes a fours group $\overline{F} \subseteq E(C_{\overline{G}}(\bar{s}))$, where every involution in $\overline{F}$ is 2-central. Now Lemma 2.9 implies that $G \cong 2^{\cdot}M_{12}$. But also, we have $N_{\overline{G}}(\overline{F}) \cong 4^2 : D_{12}$. Let $\overline{X}$ be the normal subgroup of $N_{\overline{G}}(\overline{F})$ with $\overline{X} \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, let X be the pre-image of $\overline{X}$ in G, and let F be the pre-image of $\overline{F}$ in G. Then $X = \langle x, y \rangle$, where $F = \langle x^2, y^2 \rangle$ and $F\langle a \rangle \cong SL(2,3)$. Thus $[x^2, y^2] \neq 1$. But $[x, y] \in Z(X)$, so $[x^2, y^2] = [x, y]^4 = [x^4, y] = 1$, for a final contradiction. □

Lemma 7.7. *If $\overline{G} \cong J_2$, Suz, or Co_1 then $|Z(G)| = 2$ and $|A| = 3$, and we have $C_G(A) \cong 2^{\cdot}Alt(6)$, $6^{\cdot}U_4(3)$, or $6^{\cdot}Suz$, respectively.*

Proof. Suppose first that $\overline{G} \cong J_2$. There are two classes of involutions in $\overline{G}$, with centralizers isomorphic to either $2_{-}^{1+4} : Alt(5)$ or $2^2 \times Alt(5)$. Thus, $\overline{C}$ has a subgroup L containing a and isomorphic to $Alt(5)$, and so Lemma 2.6 implies that $Z(G) \neq 1$. There are two conjugacy classes of subgroups of order 3 in $\overline{G}$, with centralizers $3^{\cdot}Alt(6)$ and $3 \times SL(2,3)$. Suppose that $C_{\overline{G}}(\bar{a}) \cong 3 \times SL(2,3)$. In the notation of [6, Table 5.3g] (which is the same as ATLAS notation, cf. [4]) we then have $\bar{a} \in 3B$, and the table shows that there are elements in the class $3B$ which commute with elements in the class $2C$, where $2C$ is represented by an outer involution of $\overline{G}$ satisfying $C_{\overline{G}}(2C) \cong L_3(2)$. Thus $\bar{a}$ lies in a Frobenius group of order 21, and we violate Lemma 2.9. This shows that $\bar{a}$ is in the class $3A$. Now suppose that $|A| > 3$. A Sylow 3-subgroup S of G is extraspecial of order 27, and $N_{\overline{G}}(\overline{S})$ contains a dihedral subgroup D of order 8 which acts faithfully on $\overline{S}/\Phi(\overline{S})$. It follows that D acts transitively on the set of maximal elementary abelian subgroups of S, and so A contains representatives from each conjugacy class of subgroups of order 3 in G. But we have seen that A contains representatives of only one class, so in fact $|A| = 3$.

Suppose next that $\overline{G} \cong Suz$. Then $\overline{G}$ has two classes of involutions. One of these has a corresponding centralizer $\overline{C}_0$ with $O^{3'}(\overline{C}_0) \cong L_3(4)$. It follows from Theorem 6.1 that $\bar{t}$ represents the other class, with $\overline{C}$ an extension of an extraspecial group 2_{-}^{1+6} by $\Omega_6^-(2)$. By Lemma 3.13, $Z(G)$ is a direct factor of $O_2(C)$, and then Lemma 2.9 implies that $C_{O_2(\overline{C})}(\bar{a}) \cong 2_{+}^{1+4}$. Thus $C_{\overline{G}}(\langle \bar{a}, \bar{t} \rangle)$ is an extension of $\langle \bar{a} \rangle \times C_{O_2(\overline{C})}(\bar{a})$ by $\Omega_4^+(2)$, and so 2^7 divides $|C_{\overline{G}}(\bar{a})|$. This information suffices to single out the conjugacy class of $\langle \bar{a} \rangle$, and to yield $C_{\overline{G}}(\bar{a}) \cong 3^{\cdot}U_4(3)$. Let $\overline{f}$ be an element of order 5 in $C_{\overline{G}}(\bar{a})$ and set $Y = O^{3'}(C_G(f))$. Then $a \in \overline{Y} \cong Alt(6)$ or $Alt(5)$, and then Lemma 2.6 implies that $|Z(Y)| = 2$. But $Z(Y) \leqslant Z(G)$, and so $|Z(G)| = 2$.

Suppose that $|A| > 3$. One checks from the character table for $2^{\cdot}Suz$ in [4] that $C_{\overline{G}}(\bar{a})$ lifts to a completely nonsplit extension $6^{\cdot}U_4(3)$ in G, so $C_G(a) = \langle A^{C_G(a)} \rangle$. Then $[V, a, C_G(a)] = 0$, whereas $Z(G)$ is fixed-point-free on V. This contradiction shows that $|A| = 3$.

Suppose finally that $\overline{G} \cong Co_1$. Then $\overline{G}$ has three classes of involutions, with corresponding centralizers $\overline{C}_i$ $(1 \leqslant i \leqslant 3)$, where the groups $\overline{C}_i$ have the structure given as follows.

$$O_2(\overline{C}_1) \cong 2^{11} \quad \text{and} \quad \overline{C}_1/O_2(\overline{C}_1) \cong M_{11},$$
$$\overline{C}_2 \cong 2^2 \times G_2(4),$$

$$O_2(\overline{C}_3) \cong 2_+^{1+8} \quad \text{and} \quad \overline{C}_3/O_2(\overline{C}_3) \cong D_4(2).$$

Let C_i denote the inverse image of $\overline{C}_i$ in G. If $C = C_1$ we obtain a faithful quadratic module either for M_{11} or for C_1, and we contradict Lemma 7.4. Suppose that $C = C_2$. Then Theorem 5.1 implies that $Z(G) \neq 1$, and it only remains to show that $|A| = 3$. Further, it follows from Lemma 6.6 that $C_{\overline{G}}(\langle \overline{a}, \overline{t} \rangle)$ contains a subgroup isomorphic to $2^2 \times SL(3,4)$, and this serves to identify $\langle \overline{a} \rangle$ among the three conjugacy classes of subgroups of order 3 in G, and to yield $C_{\overline{G}}(\overline{a}) \cong 3 \cdot Suz$.

On the other hand, suppose that $C = C_3$. We then appeal to Lemma 3.13 to conclude that $O_2(C_{\overline{G}}(\langle \overline{a}, \overline{t} \rangle)) \cong 2_-^{1+6}$, and then also $C_{\overline{G}}(\langle \overline{a}, \overline{t} \rangle)/O_2(C_{\overline{G}}(\langle \overline{a}, \overline{t} \rangle)) \cong \Omega_6^-(2)$. This information again serves to identify $\langle \overline{a} \rangle$, among the three conjugacy classes of subgroups of order 3 in $\overline{G}$, and we again obtain $O^{3'}(C_{\overline{G}}(\overline{a})) \cong 3 \cdot Suz$. Let $\overline{g}$ be an element of order 7 in $C_{\overline{G}}(\overline{a})$. Then $O^{3'}(C_{\overline{G}}(\overline{g})) \cong L_3(2)$ or $Alt(7)$, and then Lemmas 6.3 and 4.2 yield $O^{3'}(C_G(g)) \cong 2 \cdot Alt(7)$, and $Z(G) \neq 1$. Thus, we have shown that, in any case, we have $Z(G) \neq 1$, and $O^{3'}(C_{\overline{G}}(\overline{a})) \cong 3 \cdot Suz$. The character table for $2 \cdot Co_1$ in [4] then yields $C_G(a) \cong 6 \cdot Suz$ (with no non-trivial direct factors). As in the case of *Suz*, we obtain $C_G(a) \leqslant \langle A^{C_G(a)} \rangle$ if $|A| > 3$, and in that case we contradict the fact that $C_V(Z(G)) = 1$. Thus $|A| = 3$ and the lemma is proved. □

Notice that results of Lemmas 7.2 through 7.6 yield Theorem 7.1. Theorem A is then given by the union of the results Proposition 4.1, Theorems 5.1, 6.1, and 7.1.

8. Theorem B and Corollary C

Hypothesis 8.1. Assume Hypothesis 1.1 and assume also that G is not a group of Lie type in characteristic p.

By Theorem A, Hypothesis 8.1 implies that $|A| = p = 3$, and G is one of the exceptional groups listed in Theorem A. We aim first of all to determine which subgroups of order 3 in G can possibly be quadratic subgroups, with respect to some irreducible G-module V. Some of these identifications have already been made, in Lemmas 4.3, 6.6, 6.8, and 7.7. Whenever Hypothesis 8.1 is in effect, let a be a generator of A, set $\overline{G} = G/Z(G)$, and set $\overline{C} = C_{\overline{G}}(\overline{A})$. We note that, by Lemma 2.4, $\overline{A}$ is contained in a 2-local subgroup of $\overline{G}$, and we may fix a subgroup M of G, containing $Z(G)A$, such that $\overline{M}$ is a maximal 2-local subgroup of G.

Lemma 8.2. *Assume Hypothesis* 8.1, *and suppose that* $\overline{G}$ *is isomorphic to* $D_4(2)$. *Then* $\overline{C} \cong GU(4,2)$, *and* A *is contained in a subgroup* L *of* G *of the form* $(2_+^{1+6})L_4(2)$. *These conditions determine* A *up to conjugacy in* $Aut(G)$.

Proof. Identify $\overline{G}$ with $\Omega_8^+(2)$ and let U be the natural module for G over $\mathbb{F}_2$. Then $|[U, \overline{A}]| = 2^{2k}$ for some k, $1 \leqslant k \leqslant 4$. The integer k determines the structure of $\overline{C}$, and we have:

(1) If $k = 1$ then $\overline{C} \cong 3 \times \Omega_6^-(2)$.
(2) If $k = 2$ then $\overline{C} \cong GU(2,2) \times \Omega_4^+(2)$.
(3) If $k = 3$ then $\overline{C} \cong GU(3,2) \times 3$, and $\overline{A} \leqslant [\overline{C}, \overline{C}]$.
(4) If $k = 4$ then $\overline{C} \cong GU(4,2)$

The maximal 2-local subgroup $\overline{M}$ of $\overline{G}$ is a maximal parabolic subgroup. Suppose first that $\overline{M}$ is of the form $2^6 : \Omega_6^+(2)$. Then Lemma 3.13 implies that M is of the form $(2_+^{1+6})\Omega_6^+(2)$, and that $[O_2(M), A]$ is a quaternion group. Then $C_{O_2(M)}(A)$ is of order 32, and so $|\overline{C}|$ is divisible by 16. In this case we have $k = 1$ or 4. Let S be a Sylow 2-subgroup of M. There are then three maximal parabolic subgroups of $\overline{G}$ containing $\overline{S}$ and of the form $2^6 : \Omega_6^+(2)$. In the full covering group $(2^2)^{\cdot} D_4(2)$ these parabolics lift to subgroups of the form $(2 \times 2_+^{1+6})\Omega_6^+(2)$, as follows from Lemma 3.13. Since $Out(D_4(2))$ acts faithfully on the Schur multiplier of $D_4(2)$, by Lemma 3.14, it follows that, in G, two of these maximal parabolics lift to groups which are isomorphic to M, and that one lifts to a group N such that $O_2(N)$ is elementary abelian. Let M and M_1 be the two which are isomorphic to M. Then M and M_1 are fused in $Aut(G)$, and thus A is determined up to conjugacy in $Aut(G)$ in this case.

On the other hand, suppose that $\overline{A}$ is not contained in a maximal parabolic subgroup of $\overline{G}$ of the form $2^6 : \Omega_6^+(2)$. Then $k = 2$ or 3, and $\overline{M}$ is of the form $(2_+^{1+8}) : (Sym(3) \times Sym(3) \times Sym(3))$. Set $R = [O_2(M), A]$, and let V_1 be an irreducible RA-submodule of V. Then $RA/C_R(V_1) \cong SL(2,3)$, as follows from Theorem A of [3]. Set $R_1 = [C_R(V_1), A]$. If $R_1 = 1$ then $|\overline{C}|$ is divisible by 2^7, which is contrary to having $k = 2$ or 3. Thus $R_1 \neq 1$. Let V_2 be a non-trivial irreducible section for $R_1 A$ in V. Then $R_1 A/C_{R_1}(V_2) \cong SL(2,3)$. We have $Z(G) \cap R_1 = 1$, so R_1 is isomorphic to a subgroup of $\overline{R}$. As $R_1/C_{R_1}(V_2)$ is a quaternion group, it follows that $C_{R_1}(V_2)$ is elementary abelian, and then $[C_{R_1}(V_2), A] = 1$, by Lemma 4.3. Thus, $|R/C_R(A)| = 16$, and so $|\overline{C}|$ is divisible by 32. This is again contrary to $k = 2$ or 3, and the lemma is thereby proved. □

Lemma 8.3. *Assume Hypothesis* 8.1, *and suppose that* $\overline{G} \cong Sp(6,2)$. *Then* $\overline{C} \cong 3 \times Sp(4,2)$, *and this condition determines* A *up to conjugacy in* G.

Proof. There are three conjugacy classes of subgroups of order 3 in $\overline{G}$, two of which are represented in a subgroup $\overline{L}$ of $\overline{G}$ of the form $L_2(8) : 3$. Theorem 1.1 implies that $\overline{A} \not\leqslant \overline{L}$, so the conjugacy class of A in G is uniquely determined. Let U be the natural module for $\overline{G}$ over $\mathbb{F}_2$, and let b be an element of order 3 in $L - E(L)$. Then b lies in a Frobenius subgroup of L of order 21, and hence $|[U, \bar{b}]| = 16$. Let c be an element of order 3 in $E(L)$. Then c is contained in a cyclic group of order 9, and so $[U, \bar{c}] = U$. Thus, $[U, \bar{a}]$ is of order 4, and the lemma follows. □

Theorem B now follows from the results of Lemma 4.3 (concerning the alternating groups), Lemma 6.6 (concerning $2^{\cdot}G_2(4)$), Lemma 6.8 (concerning the groups $PGU((n,2))$), Lemma 7.7 (concerning $2^{\cdot}J_2$, $2^{\cdot}Suz$, and $2^{\cdot}Co_1$), Lemmas 8.2, and 8.3.

We end this section with the proof of Corollary C. Thus, assume Hypothesis 8.1, and assume that $|A|^2 \geqslant |V/C_V(A)|$. That is, assume that $|V/C_V(A)| \leqslant 9$. Denote by $\mathcal{L}$ the set

of all pairs (L, B) where L is a quasisimple subgroup L of $C_G(A)$ and B is a G-conjugate of A contained in L, with $B \not\leqslant Z(L)$. Then $[V, A, B] = 0$, and so AB acts quadratically on V. This is contrary to Theorem B, so $\mathcal{L}$ is empty.

If $G \cong PGU(n, 2)$ with $n \geqslant 5$ then the conditions given by Lemma 6.8 guarantee that $\mathcal{L}$ is non-empty. This will also be the case if $\overline{G} \cong Alt(n)$ with $n \geqslant 8$, by Lemma 4.3. If $\overline{G} \cong D_4(2)$ or $Sp(6, 2)$, we again get $\mathcal{L}$ non-empty, by Lemmas 8.2 and 8.3. Suppose that $\overline{G} \cong Co_1$. Then $\overline{C} \cong 3^{\cdot}Suz$, and $\overline{A}$ is not contained in the center of a Sylow 3-subgroup of G. Then $\overline{A}$ is not weakly closed in $\overline{C}$ with respect to $\overline{G}$, and so $\mathcal{L}$ is non-empty in this case as well. Thus, none of these cases occur.

We have $2^{\cdot}Suz \geqslant 2^{\cdot}G_2(4) \geqslant 2^{\cdot}J_2$, and this descending series of groups corresponds to a descending chain of values for $\overline{C}$: $3^{\cdot}U_4(3) \geqslant SL(3, 4) \geqslant 3^{\cdot}Alt(6)$. These conditions guarantee that the class of quadratic elements in $2^{\cdot}Suz$ restricts to the class of quadratic elements in the groups farther down the chain. Thus, to eliminate these groups it will suffice to eliminate the case $\overline{G} \cong J_2$. In that case $\overline{A}$ is contained in a subgroup $\overline{M}$ of $\overline{G}$ of the form $(2^{1+4}_{-})Alt(5)$, where the extension is split. Thus, A is contained in a subgroup K of G with $K \cong SL(2, 5)$ and with $Z(K) \leqslant Z(G)$. Then $C_V(Z(K)) = 0$, and V is a direct sum of 2-dimensional subspaces V_i, $1 \leqslant i \leqslant m$, where each V_i is an irreducible module for a fixed quaternion subgroup K_1 of K. We may choose K_1 to be A-invariant, so $m \leqslant 2$. But evidently $G \not\leqslant SL(4, 3)$, so we have a contradiction at this point.

It remains to consider the cases $\overline{G} \cong Alt(n)$, $n = 5$ or 7. In these cases, there is an A-invariant quaternion subgroup K_1 of G with $Z(K_1) = Z(G)$, so we obtain an embedding of G in $SL(4, 3)$. As 7 does not divide the order of $SL(4, 3)$ we conclude that $n = 5$, and then Lemma 2.1 implies that V is a natural $SL(2, 9)$-module for G. This completes the proof of Corollary C.

9. Examples

As mentioned in the introduction, the classification of the irreducible quadratic modules for $2^{\cdot}Alt(n)$ is given in [10], where it is shown that all such modules are "spin modules" and that all spin modules are quadratic. In this section we will show, by example, that all of the groups mentioned in parts (a) and (c) of Theorem A have quadratic modules. In order to do this, it will be convenient to have available the information given by the following lemma.

Lemma 9.1. *Let X be an extraspecial 2-group, expressed as the central product of subgroups X_i, $1 \leqslant i \leqslant n$, where each X_i is a quaternion group or a dihedral group of order 8. Let F be a field of characteristic different from 2, and let U be a faithful irreducible module for X over F. Then the following hold.*

(a) *The module U is uniquely determined up to isomorphism. It has dimension 2^n, and it is the tensor product module $U = U_1 \otimes \cdots \otimes U_n$, where U_i is the (unique) faithful 2-dimensional module for X_i over F.*
(b) *We have $N_{GL(U)}(X)/C_{GL(U)}(X) \cong Aut(X)$.*

(c) *If the characteristic of F is* 3, *and a is an automorphism of X such that $[X, a]$ is a quaternion group, then a induces an F-linear automorphism of U with $[U, a, a] = 0$, and with* $\dim([U, a]) = 2^{n-1}$.

Proof. Each X_i has four linear characters and one irreducible character of degree 2. Since F is a splitting field for X_i, there is then a unique faithful irreducible representation of X_i over F, and it has degree 2. Any irreducible representation of X over F factors through a representation of the direct product $X_1 \times \cdots \times X_n$, and is therefore a tensor product of irreducible representations of the groups X_i. If the representation is also faithful then each of its tensor factors is faithful, and so (a) holds. Part (b) is immediate from the uniqueness of U. Let a be an automorphism of X such that $[X, a]$ is a quaternion group. Then $|a| = 3$, and (b) implies that a induces a non-trivial automorphism of U over F. Here $[X, a]$ commutes with $C_X(a)$, by the Three Subgroups Lemma, and so we may take $[X, a] = X_1$. The tensor decomposition in (a) then implies that U is a direct sum of isomorphic two-dimensional modules for the group $L = \langle a^X \rangle = [X, a]\langle a \rangle$. Here $L \cong SL(2, 3)$, and if F has characteristic 3 then a acts quadratically on each irreducible L invariant summand of U. This yields (c). □

Now for the examples.

$G = PGU(n, 2)$ Let X be the central product of n quaternion groups. Then the semidirect product $K = X : GU(n, 2)$ is contained in a maximal parabolic subgroup of $SU(n+2, 2)$. It follows from the preceding lemma that there is a quadratic module U for K, of dimension 2^n over $\mathbb{F}_3$.

$\overline{G} = D_4(2)$ *or* $Sp(6, 2)$ Take $G = 2^{\cdot}D_4(2)$. Then G is the commutator subgroup of the Weyl group of the E_8-root lattice Λ. Set $V = \Lambda/3\Lambda$. Then G acts faithfully on V. Choose a maximal subgroup M of G, of the form $(2_+^{1+6})\Omega_6^+(2)$, and let A be a subgroup of order 3 in M, such that $[O_2(M), A]$ is a quaternion group. By Lemma 9.1, we may identify V with the unique faithful irreducible module for $O_2(M)$, and A acts quadratically on V.

We may identify $\overline{G}$ with $\Omega_8^+(2)$, in such a way that $\overline{A}$ centralizes a 6-dimensional non-degenerate subspace of the natural $\mathbb{F}_2$-module U for $\overline{G}$. Let $\overline{G}_0$ be the stabilizer in $\overline{G}$ of a non-singular point in U. Then $\overline{G}_0 \cong 2 \times Sp(6, 2)$. Let G_1 be the inverse image in G of the commutator subgroup of $\overline{G}_0$. Then $A \leqslant G_1$, and since A acts quadratically on V, Theorem 1.2 implies that $G_1 \cong 2^{\cdot}Sp(6, 2)$.

$\overline{G} = Co_1$, *Suz*, $G_2(4)$, *or* J_2 Next consider the case where Λ is the Leech lattice and where $G = 2^{\cdot}Co_1$—the automorphism group of Λ. Again, take $V = \Lambda/3\Lambda$. Then G acts faithfully on Λ. Let M be a maximal subgroup of G, such that $\overline{M}$ is of the form $(2_+^{1+8})D_4(2)$. Then Proposition 4.1 implies that $Z(G)$ is a direct factor of $O_2(M)$. There then exists a subgroup A of M, of order 3, such that $[O_2(M), A]$ is a quaternion group. Let R be a complement to $Z(G)$ in $O_2(M)$, chosen so that R is invariant under an elementary abelian subgroup E of M of order 81. Then R is generated by four conjugates of A, and $R = [R, E]$. Set $W = [V, Z(R)]$. Then Lemma 9.1 implies that $\dim(W) \geqslant 16$ and that A acts quadratically on W, with $\dim([W, A]) = 1/2 \dim(W)$. We now have $\dim C_V(Z(R)) \leqslant 8$, and evidently

neither $M/Z(R)$ nor $M/Z(R)Z(G)$ has a faithful representation of degree 8 over $\mathbb{F}_3$. Thus $C_V(Z(R)) = C_V(R)$, and then also $[V, Z(R)] = [V, R]$. This implies that both $C_V(R)$ and $[V, R]$ are M-invariant, and so R is normal in M. As $Z(G)$ is not a direct factor of G, it now follows from Gaschütz's Theorem that M/R is a non-split central extension of $D_4(2)$, and thus M has a subgroup K with $K \cong 2^{\cdot}D_4(2)$, and with $A \leqslant K$. As $[V, R]$ is a quadratic module for K, Theorem 1.3 implies that A is contained in a subgroup N of K of the form $(2_+^{1+6})L_4(2)$, where $[O_2(N), A]$ is a quaternion group. Then Lemma 9.1 implies that $\dim(C_V(R)) = 8$, that A acts quadratically on $C_V(R)$, and $\dim([C_V(R), A]) = 4$. Then also $\dim([V, R]) = 16$, $\dim([V, A]) = 12$, and A acts quadratically on V.

We now have $C_G(A) \cong 6^{\cdot}Suz$, by Theorem 1.2. Then A is not contained in the center of a Sylow 3-subgroup of G, and so there exists a subgroup G_1 of G with $G_1 \cong 6^{\cdot}Suz$, such that $A \leqslant G_1$ and $A \notin Z(G_1)$. Set $V_1 = [V, Z(G_1)]$. As $Z(G_1)$ is conjugate to A, we have $\dim(V_1) = 12$, and V_1 is then a quadratic module for $G_1/O_3(G_1)$. There are subgroups G_2 and G_3 of G_1, with $G_2 \cong 2^{\cdot}G_2(4)$ and with $G_2 \geqslant G_3 \cong 2^{\cdot}J_2$. By considering the structure of centralizers of elements of order 3 in the groups G_i, one finds that G_2 and G_3 contain conjugates of A, and thus V_1 is a quadratic module for G_i, $1 \leqslant i \leqslant 3$. As $O_2(G_i) = Z(G)$, for all i, all irreducible constituents for G_i in V_1 are non-trivial. As 25 divides the order of G_3 and does not divide the order of $SL(6, 3)$, we conclude that V_1 is irreducible for each G_i. Then also V is irreducible for G.

References

[1] M. Aschbacher, Finite Group Theory, Cambridge University Press, 1986.
[2] A. Borel, J. Tits, Eléments unipotents et sousgroupes paraboliques des groupes réductifs I, Invent. Math. 12 (1971) 97–104.
[3] A. Chermak, Quadratic pairs without components, J. Algebra, in press.
[4] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
[5] D. Gorenstein, Finite Groups, 2nd ed., Chelsea, New York, 1980.
[6] D. Gorenstein, R. Lyons, R. Solomon, The Classification of the Finite Simple Groups, Number 3, in: Mathematical Surveys and Monographs, vol. 403, American Math. Soc., 1994.
[7] R. Griess, Schur multipliers of the known finite simple groups II, in: Proc. Symp. Pure Math., vol. 37, 1980, pp. 279–282.
[8] R. Guralnick, K. Magaard, J. Saxl, P.H. Tiep, Cross characteristic representations of odd characteristic symplectic groups and unitary groups, Preprint.
[9] C.-Y. Ho, On the quadratic pairs, J. Algebra 43 (1976) 338–358.
[10] U. Meierfrankenfeld, A characterization of the spinmodule for $2 \cdot A_n$, Arch. Math. 57 (1991) 238–246.
[11] A.A. Premet, I.D. Suprunenko, Quadratic modules for Chevalley groups over fields of odd characteristic, Math. Nachr. 110 (1983) 65–96.
[12] B. Salzberg-Stark, Another look at Thompson's quadratic pairs, J. Algebra 45 (1977) 334–342.
[13] R. Steinberg, Lectures on Chevalley Groups, Yale University, 1967.
[14] R. Steinberg, Générateurs, relations, et revêtements de groupes algébriques, in: Colloque sur la théorie des groupes algébriques, Bruxelles, 1962, pp. 113–127.
[15] R. Steinberg, Generators, relations, and coverings of algebraic groups II, J. Algebra 71 (1981) 527–543.
[16] M. Suzuki, Group Theory I, Springer-Verlag, Berlin/New York, 1982.

[17] J. Thompson, Quadratic pairs, in: Actes du Congreś International des Matheméticiens (Nice, 1970), vol. 1, Gauthier-Villars, Paris, 1971, pp. 375–376.
[18] F. Timmesfeld, Abstract root subgroups and quadratic action, Adv. Math. 142 (1999) 1–150.